Policy Analysis

CATO INSTITUTE

January 30, 2018 | Number 831

The New National ID Systems

By Jim Harper

EXECUTIVE SUMMARY

Americans have long rejected a national ID, but many U.S. state governments are quietly developing national ID systems in a variety of forms. One is the uniform identity card system envisioned by the REAL ID Act. That federal law, passed in 2005, seeks to subject state drivers' licensing to federal data collection and information-sharing standards that will facilitate identification and tracking.

State promotion of the E-Verify background check system, which is intended to control the employment of illegal immigrants, is another path to a national ID. Successful implementation of E-Verify will require a national ID, and some states are already sharing driver data with the U.S. Department of Homeland Security so that it can be used in federally administered worker background checks.

Less well known are several other programs poised to produce the same results as a national ID without the requirement of an identity card or other formalities. These developments position states and the federal government to make once-ordinary behavior like driving on city streets and strolling the sidewalks of American towns into recordkeeping events for an overly attentive state. They compose what might be called the new national ID.

This paper summarizes the stances of each of the 50 states on various ID systems, including REAL ID, E-Verify, facial recognition, and license-plate scanning. Together, those technologies—along with other initiatives orchestrated at the federal level—are the leading edge of a national identification and tracking infrastructure.

Officials and citizens in every American state should review their states' identification, data collection, and data retention policies. The privacy and liberty of all Americans are threatened by such increasingly widespread surveillance systems.

Jim Harper is executive vice president of the Competitive Enterprise Institute and a former senior fellow at the Cato Institute. He was a founding member of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

“Systems that gather identifying information about people, along with metadata revealing their movements and activities, comprise the new national ID.”

INTRODUCTION

The past few years have seen growing awareness and concern about U.S. government surveillance of the American people. Unfolding revelations about the National Security Agency's collection of data about Americans via access to their basic communications channels have awakened many people to the increasingly real risk that the government might get—or already have—outsized ability to identify and track the populace. With that comes outsized power to influence and control.

Federal surveillance of private communications infrastructure is only one avenue along which government can monitor the private lives of citizens. Another is direct identification and tracking, such as would be possible under a national identity system. Since 2005, the federal REAL ID Act has encouraged states to combine their driver-licensing programs into a unified national ID system run by the U.S. Department of Homeland Security (DHS). Some states also require their businesses and government agencies to use E-Verify, also run by DHS, to examine the immigration bona fides of all newly hired workers. Full implementation of the E-Verify program would ultimately require a national ID system, and it continues to weave together databases of identifying information about all Americans. The threat of formal national ID systems is relatively well known, raising the question of whether the United States should have such a system.

Less well known are the many other government programs that would result in the comprehensive tracking of Americans without the use of an identity card or other formalities. State and local governments are deploying technologies such as facial recognition and license plate tracking that can observe and record the locations and movements of distinctly identified people, collecting and storing information about their comings and goings. Such programs position governments to make once-ordinary behavior like driving on city streets and strolling the sidewalks of American towns into recordkeeping events for an overly attentive state. Systems that gather identifying information about people, along with metadata revealing their movements and activities, together comprise what might be called the new national ID. These programs are on a trajectory to produce surveillance and tracking that is just as consequential and worrisome as the federal government's surveillance and formal national ID programs.

A national identity system works against the interests of free people and a free society in several ways. One is by undercutting individuals' privacy. A widely used identification system makes the collection of identity information easier and less expensive, so that governmental and corporate bodies collect more records of people's actions and movements. Whether directly or by inference, that recordkeeping exposes more to data holders about people's relationships, business activities, political leanings, social life, sexuality, and more. A national ID system undercuts the important background privacy protection of practical obscurity: the difficulty of learning about people when records are not created or when data are difficult to access or interpret.

Privacy is not just a feeling of seclusion or information control. It is also a protection for personal power. National ID systems help shift power from individuals to institutions. While providing some genuine benefits and protections, extensive databases of information also render people more susceptible to the influence or control of data holders. By learning where people have been, what they buy, with whom they associate, what their assets are, and where they can be found, for example, data holders acquire greater power. Businesses have greater ability to influence people using targeted and tailored marketing, for example. More important and worrisome, comprehensive databases of personally identifiable information give governmental authorities greater ability to exercise dominion over people and their property. People's activities are easier for the government to monitor. Their commercial dealings are clearer to authorities. Their transgressions are easier for government agents to discover.

People and their assets are easier to find and commandeer. These abilities give government greater power to control.

HOW A NATIONAL ID SYSTEM WORKS

One might be inclined to think that U.S. state programs cannot create a national ID system. They can. A national ID system has three elements:

- it is used for identification
- it is nationally uniform in its key elements
- its possession is either practically or legally required.

The first element of a national ID is that it is used for identification. This concept is simple, but there are some more complex subtleties. An identification card or system shows that a physical person now under observation is the same as someone who has been identified previously. A national *identifier* such as the Social Security number is not a full-fledged identification system. The Social Security number correlates names to numbers without making a biometric tie between the number and a physical person. In contrast, the new national ID systems either identify people or things very closely associated with people. They distinctly identify individuals directly from their license plates, which easily correlate with records about people in other databases, or through the contours of their faces. From the observation of people at certain times and places, strong inferences can be made about their lives and livelihoods, their predilections and politics.

As to the second element, national uniformity, the question is not whether one government runs the system, but whether the system runs nationally. Different jurisdictions across the country may procure facial recognition systems from different companies. If the systems use the same algorithms to distinctly identify people, they are nationally interoperable.

The third hallmark of a national ID is that its possession or use is either practically or legally required. An identity card that everyone must carry is obviously a national ID card. A card or system that is one of many options for proving identity or other information is not a national ID if people can decline to use it and still easily access goods, services, or infrastructure. This option is the case with credit cards, other payment cards, checks, and cash—among which there are many choices. If law or regulation makes it very difficult to avoid carrying a card or using the system, the card or system is in the national ID category.

The new national ID programs intersect subtly with this prong of the national ID definition. In the new national ID, nobody necessarily presses a card into anyone's hands. Nobody creates a system of incentives that encourage people to adopt the system. Rather, the system adopts the people. Camera networks in DMV offices and on the streets of towns and cities capture identifying information and collect it in databases for later use. Simply going about one's daily business subjects the individual to participation in the identity system. The only way a person can avoid it is by obscuring one's face and license plate, which is at least impractical and often illegal.

PROTECTING SAFETY VS. PROTECTING LIBERTY

Recognizing the threat to liberty, Americans have consistently rejected national identity systems that take the form of a card people might have to carry and produce in response to demands for "papers, please." Soviet-style papers and passbooks may be things of the past, but the cameras and other sensors springing up in cities and towns all over the country may be the vanguard of the far more intrusive new national ID.

Americans should ask what their state and local governments are doing with high-tech tracking, as well as whether safety and security claims used to justify tracking technology outweigh the privacy, liberty, and dollar costs of these systems. Some states have taken steps to control collection, retention, and sharing

"One might be inclined to think that U.S. state programs cannot create a national ID system. They can."

> "In effect, adopting REAL ID will create a unified, nationwide database of drivers' information."

of the data about innocent Americans they collect while operating high-tech safety and security systems. These policies should be strengthened in the states where they exist and adopted in the states where they do not.

The pages that follow examine briefly the stances of each of the 50 states toward the well-recognized national ID systems and the technologies that make up the new national ID. It is only a snapshot, and many policies are currently under debate and rapidly changing.

REAL ID AND E-VERIFY

All states collect data about their residents so they can license drivers. State databases contain photographs and vital information about drivers, such as age, birthdate, Social Security number, physical descriptors, home address, and so on. Far too many states are beginning to comply with the federal REAL ID Act, which will require them to share this information across a nationwide network.[1] In effect, adopting REAL ID will create a unified, nationwide database of drivers' information.

To facilitate this sharing, REAL ID–compliant states are expected to adopt uniform standards for collection and storage of driver information and display of driver data on the license in a standard machine readable zone. That oblique language in the REAL ID law refers to the barcodes now seen on many licenses. But in the future, it could be any technology, including radio frequency identification. Until recently, several states consistently rejected the adoption of REAL ID standards, thwarting proponents' goals in the near term.[2] But every state is now complying in some degree with the DHS's REAL ID mandates.

A parallel development is E-Verify, the national employment verification system. E-Verify's design and goals are simple. It is meant to allow employers to run the name and Social Security number of new hires through a system run jointly by the Social Security Administration and DHS, receiving confirmation or nonconfirmation of the employee's work eligibility. Essentially, E-Verify is meant to let an employer know if the employee is in the United States legally and if said employee is able to work legally, with the goal of turning off the "jobs magnet" and ending the employment of unauthorized workers in the country.

E-Verify does not deliver the easy immigration-control results it promises.[3] The program is inaccurate, frequently returning false results on American citizens/permanent residents and unauthorized workers alike. The system requires the former to prove their legal status, while the latter are erroneously judged to be work-authorized.[4] E-Verify is a threat to basic liberties, as it may trap ordinary Americans in a Kafkaesque predicament where their employment and livelihood are denied unless they prove to federal bureaucrats that they are who they say they are—without the benefit of the state-issued driver's license or ID that nearly everyone relies on.[5]

E-Verify and REAL ID originated separately, but they will not remain separate programs. An addition to the E-Verify program called RIDE (Records and Information from Department of Motor Vehicles for E-Verify) shares driver data with the E-Verify system to check the authenticity of drivers' licenses issued by states that opt in.[6] With the continued push for REAL ID by DHS and for E-Verify in conservative political circles, it is not difficult to imagine E-Verify and REAL ID becoming fully integrated so that government offices and businesses alike can be required by law to check the validity of every American's state-issued, DHS-approved REAL ID. The day would not be far off when a national ID is required for picking up prescriptions, purchasing guns and ammunition, paying by credit card, booking air travel, and reserving hotel stays, to name just a few types of transactions the federal government might regulate.

E-Verify and REAL ID both make use of photographs to identify people. The REAL ID law called only for a digital photograph and mandatory facial image capture, but many departments of motor vehicles (DMVs) are adopting facial recognition software in

tandem with their moves to comply with REAL ID. Facial recognition software analyzes the features of a person's face from a photograph, turning the facial image into a unique signature. As the technology develops, government agents will be able to run a photograph taken from a security camera, cell phone camera, or other source against a national database to see if there is a match with a base photograph already in the system (such as a standard DMV photo).[7] In a large jurisdiction like California or Texas, the DMV and law enforcement would have access to millions of photographs; with REAL ID information-sharing in place nationwide, even a small-town sheriff in rural Georgia or Vermont could have access to a database of hundreds of millions of Americans' images. And, of course, facial recognition systems could automatically scan all faces seen in a public area to look for wanted persons, incidentally gathering and keeping information about innocent persons in the area, too. Such facial recognition systems are like "papers, please" without the "please."

Similarly, an increasing number of jurisdictions are making use of license plate readers (LPRs).[8] These devices—typically mounted on police cars or integrated into traffic cameras—recognize and read license plates on passing cars, allowing law enforcement to observe the movements of all cars. Automobile license plate records are in government hands, of course, and cars are often driven by one or two people exclusively. Especially in cities with a web of cameras, license plate readers can unblinkingly pinpoint drivers' movements minute by minute, hour by hour, and day by day. Even in towns that have one license plate reader on the road into town and the road going out, the technology can record which nights a given resident comes home from work on time and which nights he or she doesn't.

Finally, several states have signed memoranda of understanding (MOUs) with the Federal Bureau of Investigation (FBI) to provide facial scans from state repositories so that states can participate in the so-called Next Generation Identification (NGI) initiative. The NGI's ostensible goal is to expand the capabilities of the Integrated Automated Fingerprint Identification System (IAFIS), the Bureau's national fingerprint check system, by integrating additional biometrics such as facial imaging, palm prints, and iris scans.[9]

States already provide fingerprint information to the FBI, and states that sign MOUs will provide the additional biometrics if—and when—they become capable. The IAFIS serves a purpose as part of legitimate law-enforcement activities, and the NGI is designed ostensibly to expand those capabilities; however, the nature of these technologies and the expanding new frontiers of biometrics raise serious questions about potential threats to the liberties of law-abiding Americans. This is because many of these technologies enable automated tracking of individuals and because they can be used to do so without any suspicion on the part of the individuals being tracked.

Together, these systems—REAL ID, E-Verify, RIDE, facial recognition, license plate readers, and the nascent NGI—are the leading edge of identification and tracking infrastructure that would significantly expand government power over citizens and residents. Assembled one piece at a time by states separately complying with federal dictates or seeking minor security gains, the endpoint of these efforts is a single system for tracking and control: the new national ID.

Officials and citizens in every American state should review their states' policies with care. Figure 1 summarizes each state's status at the time of this paper's publication with respect to formal national ID systems and the new national ID. The ID symbol in each column indicates that the state supports that part of the new national ID project. The X indicates it does not.

State policies with respect to REAL ID are subject to rapid change because of recent, aggressive DHS efforts to goad the states into implementation. Since passage of the statutory compliance deadline in 2008 without a

"The nature of these technologies and the expanding new frontiers of biometrics raise serious questions about potential threats to the liberties of law-abiding Americans."

> “Officials and citizens in every American state should review their states’ policies with care.”

single state participating in the national ID program, DHS has instituted a long series of improvised deadlines. Through the Transportation Security Administration (TSA), DHS threatens travelers from noncompliant states with refusal of their IDs when they arrive at airports. This threat puts compliance pressure on DHS’s target states, but it also pressures the agency itself, as members of Congress approach the department and its leadership with questions and criticism.

DHS’s brinkmanship typically results in some forward movement among some target states, while others hold out. The agency then succumbs to political pressure and creates a new deadline 12 to 18 months in the future. The process appears likely to repeat itself indefinitely. Enforcement of REAL ID that turns away people en masse at airports will almost certainly never occur.

The state of Nebraska is doing everything on the new national ID checklist. Maine was

Figure 1
State-by-State Participation in REAL ID, E-Verify, and RIDE; Use of Facial Recognition and License Plate Readers; States That Have Signed NGI MOUs

STATE	REAL ID	E-VERIFY MANDATE	RIDE	FACIAL REC.	LPR	NGI FACIAL SCAN MOU
Alabama	ID	ID	X	ID	ID	X
Alaska	ID	X	X	ID	X	X
Arizona	ID	ID	X	ID	ID	X
Arkansas	ID	X	X	ID	ID	X
California	ID	X	X	X	ID	X
Colorado	ID	ID	X	X	ID	X
Connecticut	ID	X	X	ID	ID	X
Delaware	ID	X	X	ID	ID	ID
Florida	ID	ID	ID	ID	ID	X
Georgia	ID	ID	X	ID	ID	X
Hawaii	ID	X	X	ID	ID	ID
Idaho	ID	ID	ID	X	ID	X
Illinois	ID	X	X	ID	ID	ID
Indiana	ID	ID	X	ID	ID	X
Iowa	ID	X	ID	ID	ID	X
Kansas	ID	X	X	ID	ID	X
Kentucky	ID	X	X	ID	ID	X
Louisiana	ID	ID	X	X	X	X
Maine	ID	X	X	X	X**	X
Maryland	ID	X	ID	ID	ID	X
Massachusetts	ID	X	X	ID	X	X
Michigan	ID	ID *	X	ID	ID	X

State-by-State Participation in REAL ID, E-Verify, and RIDE; Use of Facial Recognition and License Plate Readers; States That Have Signed NGI MOUs

STATE	REAL ID	E-VERIFY MANDATE	RIDE	FACIAL REC.	LPR	NGI FACIAL SCAN MOU
Minnesota	ID	ID *	X	ID	X	X
Mississippi	ID	ID	ID	ID	ID	X
Missouri	ID	ID *	X	X	ID	X
Montana	ID	X	X	ID	X	X
Nebraska	ID	ID *	ID	ID	ID	ID
Nevada	ID	X	X	ID	ID	X
New Hampshire	ID	X	X	X	X	X
New Jersey	ID	X	X	ID	ID	X
New Mexico	ID	X	X	ID	ID	X
New York	ID	X	X	ID	ID	X
North Carolina	ID	ID	X	ID	ID	ID
North Dakota	ID	X	ID	ID	X	X
Ohio	ID	X	X	ID	ID	X
Oklahoma	ID	ID	X	X	ID	X
Oregon	ID	X	X	ID	ID	X
Pennsylvania	ID	ID *	X	ID	ID	X
Rhode Island	ID	X	X	ID	ID	X
South Carolina	ID	ID	X	ID	ID	ID
South Dakota	ID	X	X	ID	ID	X
Tennessee	ID	ID	X	ID	ID	X
Texas	ID	ID	X	ID	ID	ID
Utah	ID	ID	X	ID	ID	ID
Vermont	ID	X	X	ID	ID	X
Virginia	ID	ID *	X	X	ID	X
Washington	X	X	X	ID	ID	X
West Virginia	ID	X	X	ID	ID	X
Wisconsin	ID	X	ID	ID	ID	X
Wyoming	ID	X	ID	?	X	X

* Indicates that the state imposes a mandate for public-sector employees and government contractors but not for the private sector. ** Indicates that Maine operates a license plate reader system; however, the system is tightly constrained by state law. See the Maine summary for further information.

Source: Created by author from sources cited in the text.

Note: RIDE = Records and Information from Department of Motor Vehicles for E-Verify; LPR = license plate readers; NGI MOUs = Next Generation Identification memoranda of understanding.

"The state of Nebraska is doing everything on the new national ID checklist."

> "With the passage of legislation in May 2017 to make Alaska compliant with the REAL ID Act, the privacy of Alaska drivers is receding."

doing none of them until it recently capitulated to DHS pressure for REAL ID compliance. Oregon has nation-leading protections for the data it collects. Below, each state's national ID and privacy practices are briefly summarized and discussed.

THE STATE OF THE STATES

Alabama

Alabama has a rather poor reputation on privacy issues and data protection, historically. The state has a complicated, and even tragic, history with the surveillance of civil rights activists and opponents of segregation during the 20th century. While Jim Crow is formally dead and buried, the state could do more to steel itself against tracking systems that could be used wrongfully in an uncertain future.

Since 2014, Alabama's Criminal Justice Information Center (ACJIC) has owned and operated at least seven mobile license plate readers. Local police forces also make use of LPR technology, including the Jefferson County Sheriff's Office and the Auburn Police Department. The involvement of the ACJIC, an adjunct of the state police that provides data to and networks with local law enforcement, allows for the sharing of captured information between multiple agencies, thereby creating multiple risks to Alabamans' privacy.[10]

In addition to being compliant with the federal REAL ID Act and all that entails for driver's license standards and information collection, Alabama's law-enforcement agencies have begun a little-noticed test program of facial recognition software.[11] Calhoun and Madison Counties have both implemented test facial recognition systems in their county jails. Analyzing 40,000 data points on an inmate's face and using 3D snapshots, the technology matches the target's image against a preexisting image in a database.

The technology is used by corrections officers in the booking and release processes to protect "officer safety" and to ensure that the incoming or outgoing inmates are who they are supposed to be. While some might not be as concerned about the liberties of criminals, Calhoun County Sheriff Larry Amerson's long-term goals should give everyone pause. The sheriff calls for making his county a hub through which all counties will link and share their own facial recognition databases—thus creating a statewide network. Nor does he wish to limit the program to jails and corrections: in the long term, the sheriff wishes to make the system mobile and use it as part of traffic stops and other police actions.[12]

Combined with the state's full-throated embrace of both REAL ID and E-Verify, as well as its notoriously difficult records-disclosure provisions, facial recognition presents an expanding threat to Alabamans' liberties. Conversely, the state has robust statutory protections against surveillance and information collection in places where there is an expectation of privacy (at home, in a public restroom, in a locker room, and so on).[13] Surveillance is permissible in public areas, however, and could involve facial recognition in the future.

Alaska

The "Last Frontier" has developed a reputation for tough, pioneer, live-and-let-live libertarianism, and rightly so. Alaska has some of the strongest privacy protections in the nation, and it is one of only 10 states to include an explicit guarantee of privacy in its current state constitution. Article 1, Section 22, of the Alaska constitution bluntly states, "The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this action."[14]

Cases before the Alaska Supreme Court have expanded upon the right to privacy. Its 1972 decision in *Breese v. Smith* found that "at the core of this concept [of liberty] is the notion of total personal immunity from governmental control: the right 'to be let alone.'"[15] *Roberts v. State* (1969) noted that the state constitution's protections on privacy were greater than those of the federal Constitution, and that the court was not "bound in expounding" privacy by the decisions of the "United

States Supreme Court, past or future, which expound identical or closely similar provisions of the United States Constitution."[16] *Ravin v. State* (1975) held that the privacy section protected the right of individuals to possess a small amount of marijuana for personal consumption in their abode.[17]

Statute law contains further protections. There are protections against license plate capture, for example, as well as against maintaining DNA in the state's DNA database if charges against the data subject are dropped, dismissed, or expunged.[18] Although the state does not have a statutory prohibition on facial recognition software, fingerprint and iris scans, or other biometric databases, successive sessions of the state legislature since 2010 have seen the introduction of bills to that effect.[19] These efforts have yet to pay off; currently, the state DMV uses a facial recognition system as part of its licensing regimen.[20] With the passage of legislation in May 2017 to make Alaska compliant with DHS's current requirements under the REAL ID Act, the privacy of Alaska drivers is receding.[21]

Arizona

Like Alaska, Arizona's state constitution contains a privacy provision. Article 2, Section 8, reads, "No person shall be disturbed in his private affairs, or his home invaded, without authority of law."[22] However, Arizona's record on privacy is far weaker than Alaska's. Arizona has been REAL ID compliant since March 2016, offering as a default voluntarily compliant licenses and IDs; Arizona is also a participant in the RIDE program. Arizonans who wish for noncompliant licenses and IDs must specifically request them.[23]Arizona also has in place 2007's *Legal Workers Act*, which mandates statewide use of E-Verify on new hires by all employers in the state.[24] Despite several challenges to the constitutionality of the law, it has been upheld by the federal courts.[25]

With regard to other elements of the new national ID, Arizona does not currently make use of a facial-recognition system, either by the state DMV or the various state police agencies. State police do use a license-plate-capture system (separate from the federal Drug Enforcement Agency's system that operates along the border),[26] and the state code includes a so-called stop-and-identify provision. Under Arizona law, police can detain individuals and demand that they provide their names. Refusal can lead to arrest.[27]

> "Under Arizona law, police can detain individuals and demand that they provide their names and addresses and explain their actions."

Arkansas

Arkansas has a mixed record when it comes to privacy and the new national ID systems, like several other states in the South. Although the state has developed through case law some protections on activity in the privacy of one's home[28] and the right to protect *some* of one's information from both private entities and government, it has also refused to allow the removal of DNA from the state DNA database following an exoneration, for example.[29]

Statute law is mixed, as well. For example, the state bans[30] private entities from operating license-plate-capture technology, while allowing state law enforcement to use the technology.[31] An ongoing civil suit from two large producers and operators of the technology asserts a violation of the companies' First Amendment rights by the state; the state, in turn, asserts that it is protecting the privacy of citizens—while operating a system of its own.[32]

Arkansas is compliant with the DHS's current REAL ID requirements. The Arkansas DMV maintains a facial recognition database for licensing purposes. But this database is not just for licensing: it is also accessed by the Arkansas Crime Information Center (an arm of the state police).[33] A routine traffic stop could see a driver's license plate scan and the driver's face run through a database for something as minor as speeding.

California

As by far the most populous state in the union, California is often a test-bed for ideas that will, in time, spread to other states. California is often at the forefront of policy debates. And when it comes to privacy and

"California makes heavy use of license-plate-capture technology."

identification, the Golden State is a leader, in ways both good and bad.

Article 1, Section 1, of the California constitution—its Declaration of Rights—has guaranteed, since a 1972 revision, an inalienable right to "pursuing and obtaining safety, happiness, and privacy."[34] The state Supreme Court has used the privacy clause to strike down restrictions on abortion, undercover police stings in schools, and discriminatory zoning laws, and also to protect financial information during the course of civil suits.[35] As in Alaska, the state courts have found an explicit guarantee of privacy under the state constitution greater than that in the federal Constitution.[36]

California's contemporary privacy record is mixed. The state has recently moved to become compliant with REAL ID (it will spend at least $220 million and hire 715 bureaucrats to do so)[37] but a 2011 state law prohibits municipalities from implementing Arizona-style E-Verify mandates.[38] California does not use a facial recognition system for law enforcement, and the state does not have a stop-and-identify law, which would require a stopped person to state his or her name and address and to explain his or her current activities. These are all strong positives.

The state does, however, make heavy use of license-plate-capture technology. California was one of the earliest adopters of the technology, with some Southern California jurisdictions operating first-generation systems in the early 2000s.[39] The three largest police forces in Los Angeles County—the Los Angeles Police Department, the Long Beach Police Department, and the county sheriff's office—have more than 400 capture devices either in use or in the midst of the procurement process, creating a huge node on the new national ID system in the state's most populous county.

Colorado

Colorado has a somewhat strong libertarian image, albeit one with more than a few blemishes. In addition to being at the forefront of the marijuana legalization movement, the state has largely rejected a broad E-Verify mandate. Colorado does mandate the use of the federal verification program or its state-run, Colorado-equivalent (the Department Program) for state contractors, a policy largely in line with the federal government's requirements for federal contractors. Private employers are free to use or not use the systems, but they are not mandated either way.

Colorado's DMV and police do not use facial recognition technology, although there has been some discussion of doing so by the DMV.[40] Several jurisdictions in the state—including Denver, Boulder, and Colorado Springs—make use of license-plate-capture systems, and several counties and municipalities have applied to DHS for program grants.[41] A slight silver lining is that Denver's police store captured information for only 21 days, so long as it is not deemed pertinent to an ongoing investigation.

Colorado also uses a stop-and-identify law, and its record on other privacy and ID issues is spotty, at best. The state has been considered compliant with DHS REAL ID requirements since 2012. Its first gold-star licenses—marked as such to indicate that identity documents are compliant—were issued in 2011.[42] Colorado has more work to do when it comes to protecting residents' privacy from the new (and old) national ID systems.

Connecticut

Connecticut has a less-than-stellar record because of its compliance with federal programs that trample privacy. Connecticut was one of the early adopters of the federal REAL ID program, and it remains one of the only states in New England to be considered fully compliant by DHS. In hand with REAL ID, the state uses facial recognition software as part of its licensing process, thus maintaining a database of driver images that can be accessed by police with a warrant.

Additionally, the Nutmeg State uses license-plate-capture systems in several jurisdictions. The state police make use of the technology as well. A Connecticut U.S.

Citizenship and Immigration Services (ACLU) Freedom of Information request found that, from 2009 to 2012, 10 towns alone in the central part of the state captured more than six million scans of plates.[43] Unlike state police, who must dump nonpertinent plate scans after 90 days, local jurisdictions operate under no such limits. In a small town like Newington (population approximately 30,000), the police can hold onto their 612,000 plate captures indefinitely.[44] That threatens the liberties of the town's inhabitants, all state residents, and Connecticut's visitors.

Delaware

Like Connecticut, Delaware scores rather low when it comes to the protection of citizens' privacy and high when it comes to creating new, pervasive forms of identification. The First State has been an enthusiastic adopter of the federal REAL ID Act and all the new standards that the law entails. With a driving population as small as Delaware's, that state stands a good chance of shortly having the largest percentage of drivers with REAL ID licenses—and all their associated information stored by the state DMV. This process includes the use of facial recognition software and other biometric markers.[45] All these methods come in handy when a citizen is pulled over as part of a routine traffic stop or is stopped by police under the state's stop-and-identify law.[46]

Delaware's status as one of the smallest states and as a state with a relatively high population density has the effect of concentrating problems. The Delaware turnpike (the state's major and unavoidable thoroughfare) alone has 162 publicly acknowledged cameras along its 13.68 miles, or roughly 12 cameras per mile. This placement goes hand in hand with the state police force's heavy use of license plate capture. If you're in Delaware and driving, chances are good that law enforcement can easily figure out who you are and where you are.

Florida

Like Alaska, Arizona, and California, Florida's constitution contains explicit guarantees of privacy. Article 1, Section 12, prohibits unlawful searches and seizures and "the unreasonable interception of private communications," unless conducted in line with the provisions of the Fourth Amendment to the federal Constitution and rulings of the federal Supreme Court.[47] Section 23 provides that "every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."[48]

The sentiments are noble, but Florida's loyalty to them is mixed. On REAL ID, the state is fully compliant, with the federal law's requirements literally written into the state code.[49] State agencies operating under the direct auspices of the governor (the majority of the state's executive branch) are required to make use of E-Verify, as are government contractors; other public agencies not under the governor's direct authority are strongly encouraged to do so.[50] Additionally, Florida is one of the first states to have signed on to the federal government's E-Verify RIDE program, which shares state data with the federal government so that employers can view driver's license and ID photos during the verification process.[51]

The Florida DMV uses facial recognition software as part of the driver-licensing process. Law-enforcement agencies ranging from the state police and the Department of Corrections to the Miami–Dade County Sheriff and rural police forces also use the software.[52] A traffic stop by a state trooper in rural Florida or a stop of a pedestrian under the state's stop-and-identify law might end up with a citizen's image run through the database. The extent of Florida's embrace of the technology is unsurprising, given the state's role as a charter member of the Facial Identification Scientific Working Group (FISWG), an arm of the FBI's oddly named Biometric Center of Excellence (BCE).[53] In 2014, the last year for which clear numbers are readily available, the BCE received at least $44 million in funding from the FBI's nearly $9 billion budget.[54]

"The Florida DMV uses facial recognition software as part of the driver-licensing process."

> "After first rejecting compliance with REAL ID, Hawaii backpedaled and implemented the federal standards."

License plate capture runs rampant in Florida, too. Jurisdictions large and small use the technology to collect license plate numbers, locations, and times without reference to any criminal suspicions. Boca Raton's three cameras (two mobile and one fixed) alone recorded more than a million plate captures from August 2010 to August 2013.[55]

Private companies in Florida operate similar systems, often for tracking down drivers who have failed to pay their car loans or payments.[56] The ability of private parties to observe and record information is not as concerning as the same activity carried out by public entities, but the public policy that requires display of license plates could be revisited in light of technology to track them.[57] Floridians need to be wary, though, of privately collected data being turned over or sold to government for use in law enforcement and less legitimate coercive activities.

Georgia

Like its neighbor to the south, the Peach State has a complicated relationship with its citizens' right to privacy and freedom from overly intrusive ID technology. Georgia has a stop-and-identify law on the books, and it is a REAL ID–compliant state, with facial recognition added in. Facial recognition is not just limited to the DMV; certain state law-enforcement agencies also use the technology. The state Department of Corrections was an early and enthusiastic adopter, implementing a system for inmate intake and release as early as 2004.[58] State law allows state and local police to access the DMV's databases as part of an ongoing investigation, handing law enforcement a ready-made database.[59]

On E-Verify and license plate capture, Georgia also falls short of the high standard for privacy practices set by some other states. Georgia is one of the few states to mandate that all employers, both public and private, use federal employment verification for all new hires, ensuring that many—and, eventually, all—Georgians are verified for work authorization by the federal government.[60] On the issue of license plate capture, the state police and large metropolitan forces (including Atlanta's, the largest in the state) have used capture technology for several years.[61] A recent case before the state Supreme Court upheld the constitutionality of using information from a capture as probable cause for a traffic stop and the arrest of a passenger for a crime unrelated to driving.[62]

Hawaii

Hawaii is one of a handful of states to explicitly enshrine a right to privacy in its constitution. Article 1, Section 6, of the Hawaii constitution states: "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right." Section 7 additionally enshrines the language of the federal Fourth Amendment's protections against search and seizure, but it does not link the content of those protections to either the federal Constitution or the federal Supreme Court (unlike Florida's similar clause).[63]

Hawaii, however, has a terrible record on citizens' privacy and ID rights. After first rejecting compliance with REAL ID, the state backpedaled and implemented the federal standards, meeting the DHS's material compliance checklist in 2013. Hand in hand with REAL ID, the state has fully embraced law enforcement's use of facial recognition technology.

Worse, the state has signed an MOU with the FBI, agreeing to assist the Bureau's effort to build the NGI biometrics database by sharing Hawaii's facial recognition database.[64] The MOU states that full implementation of the program will "permit photo submissions independent of arrests" and "permit bulk submission of photos being maintained at state and federal repositories." The FBI has also stated that it wants to use its facial recognition system to "identify unknown persons of interest from images" and "identify subjects in public datasets."[65]

In short, the FBI wants to build a national ID database, and Hawaii is doing its part. The

Electronic Frontier Foundation has filed a freedom of information suit in federal court in San Francisco, California, to get more information on just what the FBI and willing states are up to with this initiative.[66] Hawaii's participation in NGI, along with the state's use of other anti-privacy, next generation ID tools such as license plate capture,[67] should give citizens of the Aloha State pause.

Idaho

Like several other states in the Mountain West, Idaho has a robust tradition of civil libertarianism and opposition to intrusive programs. Idaho checks a number of boxes, though, when it comes to threats to privacy from identification systems. The state originally rejected compliance with REAL ID (statutorily banning compliance in 2007) and neither the state DMV nor law enforcement makes use of facial recognition software.[68] But in March 2016, legislation to comply with REAL ID was passed and signed by Gov. C. L. "Butch" Otter.[69] A handful of jurisdictions in the state make use of license plate capture, although it is not widespread statewide.[70]

A 2009 executive order from Governor Otter mandates that the state government ensure that new hires are work-authorized and requires similar verification for employees of state contractors.[71] The state—along with Florida, Iowa, Mississippi, Nebraska, North Dakota, and Wisconsin—has also joined the federal E-Verify RIDE program.[72]

Illinois

Illinois has a mixed track record on privacy and ID issues. The state constitution contains a guarantee of remedy under the law for violations of privacy, as well as a guard against unreasonable search and seizure.[73] Illinois was noncompliant with the federal REAL ID Act until recently adopting legislation to create a two-tiered, federally compliant ID system.[74]

On E-Verify, Illinois has taken arguably the strongest stance against the verification program. A 2007 law, the Right to Privacy in the Workplace Act, prohibited the use of E-Verify in the state unless and until the federal government increased the speed, security, and accuracy of the slow-moving, cumbersome system.[75] Unfortunately, that provision was struck down by a federal court in 2009. But other protections in the 2007 law survive, ensuring that the E-Verify program remains strictly voluntary in the state. Employers who choose to use E-Verify must make clear to employees all of their legal rights to privacy, nondiscrimination, and appeal.[76]

Illinois does make use of facial recognition software as part of its licensing process. The state was one of the first adopters of the technology back in 1997.[77] Several police forces, including the Chicago Police Department—the largest municipal force in the state—use the technology as well.[78] The state's branch of the American Civil Liberties Union (ACLU) cites the risk to civil liberties in Chicago, in particular, from facial recognition technology: the city government operates at least 24,000 cameras (as of 2013), all of which could be eventually tied into a networked system.[79] Combined with the state's already widespread use of license plate capture by fixed cameras and police, as well as the state's stop-and-identify laws, the threat to liberties from an integrated network of cameras and systems is strong.[80]

Indiana

While Illinois has a mixed record on privacy and ID issues, neighboring Indiana has one of the poorest records of any state. The state was an enthusiastic adopter of REAL ID, embracing the program shortly after the standards were rolled out in 2008. It was so enthusiastic, in fact, that the American Association of Motor Vehicle Administrators (AAMVA)—a DMV managers' pro–REAL ID pressure group—gave the state an award for implementation.[81] Indiana has embraced the E-Verify program, mandating its use for all new public-sector hires and government contractors, and offering a tax break for private employers who enroll.[82]

Indiana implemented a facial recognition system in conjunction with its REAL ID

"Indiana has one of the poorest records of any state."

"Kentucky had one of the better records on privacy and ID with respect to participation in federal programs, but it recently moved toward complying with REAL ID."

rollout in 2009. In addition to literally requiring that people not smile in their drivers' license photo,[83] the technology is being used by law-enforcement agencies and other agencies of the state government—including, it seems, the state gaming commission.[84] That the government body charged with regulating Indiana's casinos can access the database raises troubling questions about who else in the state can access the database and about what authority and justification are required.

Indiana's law-enforcement agencies also use license-plate-capture technology in numerous jurisdictions. Worse, individual jurisdictions set their own policies on capture and retention, with municipalities such as South Bend keeping capture data and images for up to 18 months, with the possibility of an extension.[85] State police, too, use the technology, performing more than 400,000 captures in 2013 alone.[86] A 2013 bill in the state Senate to place strict limits on how captures are obtained and how they are retained was unfortunately killed in committee.[87] The one thing Indiana does not do to make itself a new national ID state is provide state residents' DMV data to the E-Verify program through the RIDE program.

Iowa

Iowa's new national ID record is largely negative. The legislature and executive branch have rejected mandatory E-Verify legislation and executive orders, but the state has embraced REAL ID wholeheartedly.[88] Despite rejecting mandatory E-Verify so far, Iowa is one of a few states to embrace the federal government's RIDE program, making the personal information of license holders available to the federal government's employment verification systems.

Iowa has also embraced the use of facial recognition technology. The state Department of Transportation uses the technology as part of the licensing process, and police have begun to use the database of images to make arrests.[89] Mandatory image capture for sex offenders has been considered as well.[90] It is hard to oppose the technology's use on sex offenders and longtime fugitives, but it might be soon coming to all Iowans: the state Department of Public Safety, which oversees policing and security in Iowa, is interested in developing the capability to implement widespread use of recognition systems for law-enforcement purposes.[91]

Kansas

Kansas has a mixed record on national ID and privacy issues. The state legislature rejected a statewide E-Verify mandate in 2012.[92] On the other hand, Kansas is fully compliant with the DHS's current REAL ID Act requirements—indeed, the state was nearly fully compliant when the original compliance benchmarks were first rolled out.[93] The state uses facial recognition, and the data are maintained by the state DMV, ostensibly to prevent the issuance of multiple licenses to one individual.[94]

Individual jurisdictions in Kansas use license-plate-capture technology, with local police forces apparently setting their own standards for how long the data are held and who can access it. A 2012 Freedom of Information request from Kansas's branch of the ACLU to the local police department of the small town of Hutchinson shed some light on these policies.[95] Hutchinson's response to the request stated that the department kept all data until space was needed on its servers, that any officer could access the data, and that it could be shared with other forces and agencies as part of an investigation. The response stated that the Hutchinson Police Department has neither training materials for the system nor any training program at all. If Hutchinson's example is anything to go by, all Kansans should be concerned.

Kentucky

Kentucky had one of the better records on privacy and ID with respect to participation in federal programs, but it recently moved toward complying with REAL ID.[96] The state does not require use of E-Verify by public or private employers.

However, the state has maintained (since 2005) a facial recognition database that uses driver's license pictures.[97] Access to the data is limited, according to one report; only 34 DMV and law-enforcement officials can access the database.[98] The effectiveness of Kentucky's system has been questioned. The Electronic Frontier Foundation has asserted that Kentucky's system is largely useless without "sterile" conditions, requiring a suspect's picture to be at the same angle as a DMV-taken picture to return an effective result.[99] If true, Kentuckians should ask why they are paying for the system.

Louisiana

Louisiana has a mixed record on anti-privacy and ID programs. On E-Verify, the state's approach is largely governed by two 2011 laws: HB342 and HB646.[100] The bills amended state law to mandate E-Verify use for government contractors (but not public employees) and to require private employers to check their new hires' IDs. The statute recommends—but does not mandate—the use of the federal system. Louisiana does not allow automatic license plate readers; on June 19, 2015, then-governor Bobby Jindal (R) vetoed a bill that would have allowed widespread use of automatic license plate readers by law enforcement.[101]

On facial recognition systems, Louisiana is one of 13 states declining to use the technology for licensing or law-enforcement purposes. However, Louisiana is compliant with REAL ID thanks to 2016 legislation signed by Gov. John Bel Edwards (D).[102]

Worsening matters for Louisianans, the summer of 2016 saw a massive data breach of the state's driver information databases. Coinciding roughly with the state's adoption of REAL ID, more than 290,000 residents of Louisiana were apparently affected by the breach. The stolen information was typical of that which is held by motor vehicle bureaus: name, license number, state of issuance, address, phone number, email address, and driving records. Louisiana's adoption of REAL ID will make such occurrences more consequential in the future.[103]

In total, Louisiana is quite good on plate capture and facial recognition technology. One can hope that it will continue to be so in the future. On REAL ID and E-Verify, it has plenty of room to improve.

Maine

The Pine Tree State's former strong record on ID privacy took a step backward early last year with the passage of REAL ID compliance legislation. Maine's legislature passed noncompliance resolutions for REAL ID as early as 2007, and the state remained noncompliant for a long time in the face of federal efforts to force adoption of the national ID law.[104] In April 2017, the state legislature finally capitulated, passing legislation to enter Maine into the national ID system.[105] On the other big federal identification program, E-Verify, Maine does not impose a mandate on public or private workers.[106] Maine employers are free to choose whether they want to use the system.

Maine has arguably taken one of the strongest anti-facial-recognition-software stances in the country. The state does not use the technology; according to Secretary of State Matthew Dunlap, the state government prohibits its use by any state agency.[107] Only one county in the state has purchased software for its police force, and the press coverage of Cumberland County's decision to spend $35,000 on an error-ridden, privacy-trampling system has been hostile to say the least.[108]

Maine has taken similarly strong stands on the issue of license-plate-capture technology. A 2009 law places hard limits on what law enforcement and the state Department of Transportation can and can't do with plate capture data.[109] Plate captures can be only for legitimate law-enforcement purposes, the data must be kept confidential, and that information may not be stored for longer than 21 days if not part of an active investigation.[110] Maine's law is a model for other states.

Maryland

The Old Bay State has a mixed record on federal programs and a poor one on the new

"The Pine Tree State's former strong record on ID privacy took a step backward early last year with the passage of REAL ID compliance legislation."

"Americans may increasingly find themselves having to prove their identity to the government using government documents that the government asserts are fake or false."

national ID programs. Maryland does not mandate the use of E-Verify for public and private employees or for government contractors. However, it is REAL ID compliant, issuing gold-star licenses to all citizens and legal residents, though it does give non–REAL ID licenses to unauthorized aliens who can prove residency in Maryland.[111] Maryland is also a participant in the RIDE program.[112]

Maryland allows license plate reader technology to be used by law enforcement. However, the use of the technology is subject to a 2014 law that limits its usage and places restrictions on access, data use, and data retention.[113] While not perfect, the law is a step in the right direction.

However, the state put in place a facial recognition system in March of 2011. This system was originally run by the state Department of Public Safety and Correctional Services, which oversees the state police and prison system. More than 2.1 million photos of offenders and convicts were uploaded. But the database does not stop there. In December 2011, Maryland joined Hawaii and signed an MOU with the FBI, integrating the state's smaller database with the Bureau's larger database of more than 12 million photos.[114]

Some may not have many qualms about sharing perpetrator photos with the chief federal law-enforcement agency. In the spring of 2013, though, Maryland added nearly 6 million driver photos from the state's Motor Vehicle Administration to the state (and, via the MOU, to the federal) photo database. Maryland has erected a formidable surveillance system. It's not just criminals and convicts anymore who have to fear: it's millions of law-abiding Marylanders, too.

Massachusetts

Massachusetts's experiences with privacy and ID (and facial recognition, in particular) offer a fine example of the danger and the absurdity of the new national ID. That the state does not mandate or encourage the use of E-Verify is helpful, but that fact does not detract from a problematic facial recognition system.[115]

The state Registry of Motor Vehicles (RMV) maintains facial recognition software and a database of license photos, which state police can access if they make a request.[116] Recent technological advances have given county sheriffs' departments the ability to access the databases remotely, turning patrol cars into arms of a vast, networked database.[117]

The experiences of one Massachusetts resident highlight the dangers and absurdities of these programs. In 2011, John H. Gass, a law-abiding resident of Natick, received a notification from the RMV informing him that his license had been revoked. It turned out that the state's facial recognition software had flagged his license picture as a duplicate of an existing picture; apparently, Gass bore a resemblance to one of Massachusetts's other 4.6 million drivers. The innocent man was forced to go through a lengthy process of appeals with the RMV, which required that he prove to that department that he was who he said he was.[118]

Gass's experience is a hint of what may be to come under centralized governmental ID systems. Americans may increasingly find themselves having to prove their identity to the government using government documents and government-issued IDs that the government asserts are fake or false. It creates an absurd cycle, where the burden of proof is placed on the defendant (the ordinary citizen) as opposed to the accuser (the government). Gass's experience should be a wake-up call to Massachusetts and America as a whole.[119] Massachusetts signed up for REAL ID compliance in July of 2016.[120]

Michigan

Michigan has a mixed record on protecting the privacy and ID rights of its citizens. On REAL ID, DHS considers the Wolverine State technically noncompliant, but it has begun issuing federally compliant IDs, and several benchmarks have been met.[121] On E-Verify, the state has no mandate for public or most private workers, with the only mandate being imposed upon government contractors

who work with the state Department of Transportation.[122]

Michigan has not put in place facial recognition software as part of its licensing process. However, the state police force does use the technology, including mug shots, correctional facility photos, and photographs taken as part of active investigations.[123] As one of four states to sign an MOU with the FBI as part of the Bureau's NGI program, Michigan's system is connected to the federal test system. Michiganders may take solace in knowing that the program is currently confined to mugshots and pictures of criminals, but they should worry about the day when the state turns over its vast database of driver's license photos.

Minnesota

Minnesota recently moved from having a somewhat good record on privacy protection and ID issues to a decidedly mixed one. The state was long noncompliant with the REAL ID Act, even defiant of it with a ban against participation enshrined into state law in 2009.[124] However, Minnesota finally succumbed to DHS threats and adopted compliance legislation in May 2017.[125]

Use of the federal E-Verify system is only required for government contractors executing contracts of more than $50,000.[126] In 2009, former governor Tim Pawlenty (R) implemented an executive order for all new public employees to be verified; in 2011 Pawlenty's successor, Gov. Mark Dayton (D), vetoed an attempt by legislators to reimpose the mandate and allowed the order to lapse.[127]

Minnesota's law enforcement and DMV use facial recognition software. The former uses the technology in correctional facilities and to run mugshots through a database of known felons, while the latter uses it to protect against multiple-license fraud.[128] Minnesota law circumscribes how facial images can be used.[129]

That law hasn't stopped some officers and officials from abusing the system. Illicit and illegal searches of the system appear to be rampant in Minnesota. More than 8,400 verified illicit lookups of information were conducted according to an audit by state officials, revealing photographs, addresses, and driving records, typically of women who are former police officers, TV news personalities, and ex-partners of public employees.[130] Potentially 19,000 more were conducted by a single employee of the state's Department of Natural Resources. Eighteen federal lawsuits against towns and the state have been launched over the rampant abuse, and more may be in the pipeline.[131]

On the issue of plate capture, 2014 legislation included language from an earlier bill that aimed to restrict the practice. The final bill, as passed, effectively creates a 120-day limit for use of the data by the appropriate law-enforcement agency. If the captured images and data are not being used, they are reclassified as private data (as opposed to confidential data), which is more carefully protected under the law.[132] Again, this is a small protection, but it is a protection nonetheless.

Mississippi

Like neighboring Alabama, Mississippi has a poor record on ID privacy. The state is compliant with REAL ID and, to make matters worse, is DHS's lead state in a consortium studying how to better integrate state and federal information databases.[133] Mississippi mandates that all employers use the E-Verify system, and the state is also a member of the RIDE program, allowing for checks of employees' driver's licenses as part of E-Verify's verification process.

On the facial recognition front, Mississippi has one of the longest-running programs in place, first implemented in 2003.[134] In addition to integrating the state police's collection of images with those of the state's 82 county forces and numerous municipal forces, Mississippi allows law enforcement to access the state's driver's license photo database under certain circumstances. Additionally, police forces in the state use license-plate-capture technology, especially in large municipalities such as Jackson.[135]

"Minnesota finally succumbed to U.S. Department of Homeland Security threats and adopted compliance legislation in May 2017."

"Montana has done well to resist REAL ID in the past but recently moved to grudgingly comply with the national ID law."

Missouri

Missouri has recently faltered from its generally good record on privacy issues. The state was noncompliant with REAL ID (with a strict legislative ban on compliance in place),[136] but recently adopted legislation to come into compliance with the DHS's current requirements under the national ID law.[137] Missouri also has an E-Verify mandate in place for public employees and government contractors working on contracts of more than $5,000; however, there is no private-sector mandate.[138]

On the issue of facial recognition software, Missouri signed a contract with a vendor to implement a driver's license facial recognition system in 2011. In 2013, however, work on the system stopped.[139] Opposition to implementing the intrusive system surfaced in both the state House and state Senate, and the fiscal year 2014 appropriations bill for the state Department of Transportation included a clause that killed funding for any photo verification system.[140] By doing so, Missouri's legislature struck a blow for liberty.

Montana

Like several other states, Montana enshrines the right to privacy in its constitution. Article 2, Section 10, of the Montana constitution notes that "[t]he right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."[141] How, then, does the Big Sky Country stack up when it comes to privacy?

Montana has done well to resist REAL ID in the past but recently moved to grudgingly comply with the national ID law. Recent legislation gives Montanans the option of paying a fee for a special license that complies with federal requirements.[142] The state has no E-Verify mandate in place for either public or private employers. On the two state–federal collaborative programs, then, Montana until recently did very well.

At the state level, Montana uses facial recognition technology as part of its licensing process, ostensibly to prevent fraud and multiple issuances.[143] Police are unable to access the database of photos.[144] Police forces in the state do not currently use license plate readers, though, and there is a budding legislative movement against allowing the technology to be used.[145]

Nebraska

Nebraska has a poor record on privacy and ID issues. In fact, it is the one state that does everything on the new national ID list. The state is fully compliant with the current requirements of the federal REAL ID Act, adopting most of the law's provisions via 2009's LB 261.[146] Nebraska also has an E-Verify mandate in place for public-sector employees and government contractors, and the state Department of Revenue grants tax breaks to certain categories of private employers if they use the federal program.[147] Businesses are given financial incentives to embrace E-Verify, as opposed to putting in place a hard mandate. Some local municipalities (most notably, the town of Fremont) have put in place their own private sector E-Verify mandates, despite ongoing legal challenges.[148] Additionally, Nebraska is one of the few states to participate in RIDE.[149]

As part of its embrace of REAL ID, Nebraska integrated facial recognition into its licensing process in 2009.[150] State statutes prevent the dissemination of driver's license photos to any but local, state, or federal law enforcement undertaking an investigation,[151] with most requests for access routed through the Nebraska Criminal Justice Information System.[152] Nebraska has, however, entered into an MOU with the FBI for the Bureau's NGI program, providing easy access to the database for federal investigators.[153] Combined with Nebraska's various police agencies' heavy and increasing use of license-plate-capture technology, Nebraskans are unwitting participants in the new national ID system.[154]

Nevada

What happens in Vegas stays in Vegas—on video. That statement applies also to Nevada's

new national ID programs. The state deserves credit, though, for avoiding federal mandates in the past.

On REAL ID, the Silver State is currently compliant with DHS's requirements, having reversed its earlier opposition to the national ID program. The state legislature passed an anti-compliance resolution as early as 2007.[155] But in 2009, then-governor Jim Gibbons (R), a REAL ID proponent, issued an executive order to the state DMV ordering compliance. A successful lawsuit brought by the state ACLU, the Clark County Republican Party, gun rights groups, and libertarian groups killed the governor's backdoor implementation.[156] Proponents, however, tried again, and the legislature brought the state into compliance. In 2015, Nevada began issuing REAL ID–compliant licenses.

E-Verify, too, has met opposition in Nevada—an unsurprising fact in a state with a large population of native-born Hispanic Americans, who are more likely than others to encounter mix-ups in the system and discrimination from employers. The state has so far declined to put in place public- or private-sector mandates, despite the urgings and efforts of some elected officials.[157]

Nevada does, however, have in place a facial recognition system as part of the state's licensing process. The system is internal to the DMV and is typically accessed only by "sworn employees" investigating potential cases of license fraud.[158] Importantly, police do not have free access; they must submit photos to the DMV to have them run through the system.[159] It's a small protection, but a protection nonetheless.

Unfortunately, the state does use license plate reader technology, as well. The Nevada Highway Patrol (NHP) uses the technology in conjunction with the federal Drug Enforcement Agency (the state force having no tracking devices of its own). The reader units themselves belong to the Drug Enforcement Agency, with the NHP passing plate captures along to the federal agency—in effect, acting as deputies for federal law enforcement.[160] Local jurisdictions such as Boulder City, Reno, and Henderson use their own, independent readers for local law enforcement, as well.[161]

New Hampshire

If any state in the Union is associated with the ideas of liberty and government noninterference in the lives of citizens, it is New Hampshire, home of "Live Free or Die" and a flinty libertarian tradition. Unsurprisingly, New Hampshire does well on protecting the liberties and privacy of its citizens from the new national ID, though it has recently weakened. Efforts by members of the state legislature to introduce E-Verify mandates have been rejected in several sessions of the legislature, with a recent example—HB267—being ruled "inexpedient to legislate" on during the 2015 session.[162]

Additionally, state law makes the use of facial recognition scanners by the DMV and law enforcement exceedingly difficult, if not impossible. Section 260:10-b of the state code prevents the state from collecting—in conjunction with licensing or motor vehicle registration—most forms of biometric data, including facial scans and retina scans.[163] Other provisions create strict standards and regulations for law enforcement's use and maintenance of any of the biometric data that are collected as part of legitimate criminal investigations.[164]

Finally, New Hampshire does not allow the use of license-plate-capture technology. The law is clear: Section 261:75-b of the state code bluntly states, "The use of automated number plate scanning devices is prohibited except as provided in RSA 236:130."[165] The sole exceptions are when the scanning is permitted on a case-by-case basis as part of an active investigation (blocking random, roving scans) or for operating automated toll systems, among other mundane administrative tasks of the state Department of Transportation.[166] Even then, hard blocks are in place about how the data can be used, along with explicit prohibitions on transmission of data or its use for roving or illicit surveillance.

"New Hampshire does not allow the use of license-plate-capture technology."

"In late 2016, however, New Mexico adopted a two-tiered licensing system, offering both compliant and noncompliant licenses."

However, there is one black mark on New Hampshire's record: REAL ID. New Hampshire was an early state to reject REAL ID, passing a ban on implementation of the federal standards in June 2007.[167] That ban was overturned in May 2016 with the passage of HB 1616, a bill to bring New Hampshire—the birthplace of the REAL ID rebellion—into compliance with the federal ID law. Effective January 1, 2017, New Hampshire began issuing REAL ID licenses.[168]

New Jersey

New Jersey's record on privacy and ID rights is mixed, at best. For a long time, the Garden State was noncompliant with REAL ID, but that noncompliance was something of a fluke: the state was moving ahead with compliance until a court order suspended the effort. Since then, it has become clear that state officials will bring the state into line with the federal ID standards.[169] Efforts to implement mandatory E-Verify in New Jersey for all employers have failed in successive sessions of the legislature, with the same bill being introduced in 2010 and in 2014.[170]

The state has, however, implemented facial recognition software for licensing and for law enforcement. A vast review of every New Jersey facial image (creatively titled Operation Facial Scrub) was conducted between 2011 and 2013, with more than 19 million photos in the state Motor Vehicle Commission's database scanned to look for duplicates.[171] All new pictures in the database will be "scrubbed" against existing photos as they are added. As Massachusetts's problems with false matches have shown, innocent New Jerseyans will risk falling afoul of these automated scrubs.

Finally, New Jersey—famous (or infamous) for its Parkway and Turnpike—is no stranger to the use of license plate readers by state police and municipal police forces. The state's regulations relating to the use of the readers are extremely loose. A 2010 directive issued by the state attorney general limits scans to license plates on vehicles that are in public view, which is defined as "vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shopping mall or other business establishment."[172] In short, any car in New Jersey that is not parked in a closed private garage is fair game for a roving license plate reader.[173]

New Mexico

New Mexico once rejected compliance with REAL ID; the state's practice of issuing standard, undifferentiated driver's licenses to unauthorized migrant residents ensured that it could not comply with the terms of the national ID law.[174] In late 2016, however, New Mexico adopted a two-tiered licensing system, offering both compliant and noncompliant licenses.

The Enchantment State imposes no E-Verify mandates on either public or private employees.[175] Given the large Hispanic American population and the rather vocal opposition of local activists, officials, and the Catholic Archdiocese of Santa Fe to anti-immigrant ordinances, the state's reluctance to push E-Verify is unsurprising.

New Mexico does, however, have a robust facial recognition system in operation at the state DMV. The state uses the technology for law-enforcement purposes, too. To make matters worse, New Mexico is one of several states to sign an MOU with the FBI about the Bureau's NGI program.[176] Although the pictures and images that are—so far—being uploaded are mugshots, correctional facility images, and so on, it's not a huge leap to imagine New Mexico's driver's license images joining the federal government's ever-expanding database for facial recognition in the future.

New York

Like California, the sheer size of New York's population and its influence on matters of public policy give the state weight beyond that of most others. How does New York fare when it comes to protecting the privacy and ID rights of its citizens? New York's record, like California's, is complicated.

Like many, the Empire State was noncompliant with REAL ID until recently. It is now issuing gold-star licenses to make the state's driver-licensing regime acceptable to the federal government.[177] New York does not enforce an E-Verify mandate, either. The state does, however, use a robust facial recognition system as part of its licensing process. "Robust" may be understatement; the state DMV maintains a database of more than 20 million images against which every new picture is scanned. Ostensibly to fight fraud, state officials have touted 13,000 investigations and 2,500 arrests.[178]

As in New Jersey and Massachusetts, the technology raises the specter of false positives and the risk of citizens being forced to prove to the state that they are who they say they are without using their driver's licenses. As the New York Police Department (NYPD) (the largest municipal police force in the United States) and other forces begin to use facial recognition software as a policing tool, the likelihood of errors creating legal challenges and rights violations for innocent citizens grows.[179]

Unsurprisingly, too, the NYPD and other police forces have been eager adopters of license-plate-capture technology. In Manhattan, for example, it is impossible to enter or leave the borough by car without having one's license plate scanned; all of the bridges and tunnels into and out of the island are covered.[180] Mobile readers in the city and fixed-location cameras (both public and private) have given the NYPD a database of more than 16 million plate captures (as of 2013), which can be stored for up to five years and run through the city's multimillion dollar, dashboard-equipped Domain Awareness System.[181] Other cities and towns are getting on board, too, with the state earmarking roughly half a million dollars in grants to local forces for the purposes of getting their own systems.[182] Leviathan grows in New York.

North Carolina

North Carolina has a poor record when it comes to protecting the privacy and ID rights of its residents. State officials brought the state's licensing regime into compliance last year, and several of the DHS benchmarks for REAL ID compliance have been implemented.[183] If that isn't bad enough, the state also imposes an E-Verify mandate on all public and private employers.[184] The 2012 legislative session's HB36 apes federal proposals for mandatory E-Verify, with staged implementation based on the size of the employer coming fully into effect for all businesses in July 2013. An earlier bill, SB1523 in 2007, implemented a mandatory requirement for all public employees and government contractors.[185]

Unsurprisingly, North Carolina's DMV and law enforcement use facial recognition technology and license plate capture. The state was one of the earlier adopters of facial recognition technology (as early as 2004). Having signed an MOU with the FBI, it shares its vast driver and criminal databases with the federal government.[186] License plate captures are also poorly protected; a 2013 bill to regulate law enforcement's use of the technology and provide some clarity to the state's murky laws and regulations governing it died in the state Senate.[187]

North Dakota

North Dakota once rejected compliance with REAL ID, but recently made the national ID an "opt-in" program for its residents.[188] The state has not implemented E-Verify mandates for public- and private-sector employers.[189] North Dakota does, however, participate in the RIDE program, tying the state's DMV database to the (for employers) voluntary E-Verify process.[190]

The state uses facial recognition technology at its DMV and has done so since 2010.[191] Police appear to have limited access to the database, as part of the DMV's fraud prevention. License plate readers do not appear to be used in the state, although some assert that the Bismarck Police Department does—clandestinely—operate the technology; the Bismarck Police Department denies this charge.[192]

Ohio

Ohio has a mixed record on the issue of privacy and ID rights, with some spectacular

"It is impossible to enter or leave Manhattan by car without having one's license plate scanned."

"Oklahoma recently caved in an important way on protecting citizens' privacy and ID rights."

highs and lows. Ohio is the only state (so far) to embrace REAL ID, reject it, and then embrace it again. Deemed compliant by DHS in December 2012, the Buckeye State rolled back compliance, citing concerns over privacy and data protection.[193] It then reversed course again and brought Ohio's licenses into compliance once again in 2015.[194] Ohio has not imposed an E-Verify mandate, with a 2012 bill to do so dying in the legislature.[195]

Ohio runs a facial recognition system at its DMV (an offshoot of REAL ID compliance); according to one report, the state has the loosest standards in the nation for access to the database.[196] More than 30,000 state and local police officers and court employees can access the Ohio database, which was established by and is still run by the state attorney general's office (in contrast to other states, where the databases are under the purview of the motor vehicle bureau). By comparison, only 34 people in neighboring Kentucky can access that state's database, and all those who do must receive training on the system. In Ohio, there is little in the way of formal training and little in the way of checks on access. Indeed, information is shared not only with Ohio officers and government employees, but also with their federal counterparts and counterparts in other states.[197]

Little has been done to tighten Ohio's standards and practices for access and use of its facial recognition database. The potential for abuse is ripe, and Ohioans should be deeply concerned about the easy access to their personal biometric information. Ohio's lax treatment and security should also concern all Americans. As goes Ohio, so could go the whole country.

Oklahoma

Oklahoma recently caved in an important way on protecting citizens' privacy and ID rights. The state and successive gubernatorial administrations had been staunch opponents of the federal REAL ID Act, banning compliance through 2007's Oklahoma SB 464. But in early 2017, the Oklahoma legislature passed, and Gov. Mary Fallin (R) signed, legislation to bring the state into compliance with federal mandates.[198] Oklahoma also has an E-Verify mandate in the form of 2007's Oklahoma Taxpayer and Citizen's Protection Act (HB 1804).[199] The mandate applies only to public-sector workers and government contractors, however; it does not include a private-sector component.

The state does not use a facial recognition system as part of its licensing process. However, it does capture other biometric information as part of the process (namely, fingerprinting) and does use high-quality photography. Oklahoma's use of biometrics has received some outside attention from Tea Party members and religious groups because of a lawsuit brought by state resident Kaye Beach. Beach's suit objects to the biometric requirements of the state's licensing regime on the grounds of privacy and religious freedom, calling the technology the "mark of the Beast."[200]

Finally, since 2012, Oklahoma City Police—the largest municipal police force in the state—have used license plate readers, retaining the resulting data for up to 90 days.[201] The ACLU has found that three other jurisdictions—Tulsa, Norman, and Lawton—use the technology, meaning that the state's four largest municipalities (and four-largest population centers) capture license plates with little oversight.[202]

Oregon

Like the other states in the Pacific Northwest, Oregon has had a good record on protecting privacy and ID rights—with a few notable and recent hiccups. Oregon has rejected mandates for E-Verify for both public- and private-sector employers.[203] The state was firmly noncompliant with REAL ID, having banned compliance by statute in 2009, but legislation passed in July 2017 puts the state on a path to implementation of the national ID law.[204]

Oregon does use facial recognition software at its DMV. Although Oregon's facial recognition technology, collection of other biometrics, and collection of personal information seem as ominous as comparable actions in other states, the Beaver State has one thing

that most other states don't: ironclad privacy protections in the state code. Section 801.063 bars unwarranted and warrantless disclosure of DMV information to outside parties, and it explicitly bans participation in federal or multistate data sharing schemes unless and until the other jurisdictions meet Oregon's high standards for privacy protection.[205]

Oregon does a good job of protecting biometric data, and a movement is beginning to protect other forms of data. Spurred by the National Security Agency spying scandal and the revelation that Portland's police department is capturing more than 100,000 license plate images a day, legislators have considered important controls.[206]

Pennsylvania

Pennsylvania's record on privacy and ID rights is poor. Promisingly, the Keystone State rejected compliance with the federal REAL ID Act through legislation in May 2012.[207] But in the spring of 2017, it capitulated to the federal government and passed legislation to implement REAL ID, which will cost the state $27 million in the first year and between $17 million and $20 million per year thereafter.[208] Pennsylvania adopted a public-sector and government contractor E-Verify mandate almost simultaneously with its July 2012 rejection of REAL ID. That mandate imposes heavy fines and gives the state the ability to suspend business licenses for repeat failures to use the E-Verify system.[209]

Pennsylvania has, unfortunately, a facial recognition system that it uses at its DMV, despite rejecting REAL ID. To make matters worse, the state has fully integrated its driver database with state law enforcement's Justice Network.[210] The Justice Network's facial recognition system has access to every Pennsylvania driver's image, allowing 500 local, state, and federal law-enforcement agencies to access driver images. The pre–Justice Network database was accessible only to state police and the state attorney general's office. Although not as bad as Ohio's vast and easy access, Pennsylvania has drastically expanded both the scope and level of access to the biometric data of its 8.8 million drivers.

Rhode Island

The smallest state has some worrisome policies when it comes to the protection of citizens' privacy and ID rights. Not all are bad. In 2011, Gov. Lincoln Chafee (I) overturned an E-Verify mandate imposed by his predecessor in 2007.[211]

Although noncompliant for many years, the state embraced several of the benchmarks of REAL ID and went beyond it with an advanced facial recognition system and the collection of other biometric information.[212] Governor Gina Raimondo (D) recently determined to bring the state into compliance with REAL ID.[213]

Law enforcement can freely tap into the facial recognition database. There are no checks on license plate capture, the other scourge of privacy and free travel. There have been moves to make it more pervasive; two bills during the 2013 session of the Rhode Island legislature would have expanded the scope of usage by police.[214] They expired before the session ended.

Rhode Island's code allows for untrammeled storage of digital data and for the digitization of analog information. This storage includes facial information, other biometrics, Social Security numbers, tax numbers, and most other forms of personal identifiers.[215]

South Carolina

South Carolina is part of that small group of states that enshrines a right to privacy in its state constitution. Article 1, Section 10, of South Carolina's constitution is largely a restatement of the federal Fourth Amendment, guaranteeing South Carolinians protections against unreasonable invasions of privacy and promising that no searches or seizures of items or information will be conducted without a warrant issued based upon probable cause.[216]

The Palmetto State was one of the earliest states to adopt an E-Verify mandate. In June 2008, the South Carolina Illegal Immigration Reform Act was signed into law, with the

"Law enforcement can freely tap into Rhode Island's facial recognition database."

> "In April 2017, South Carolina adopted legislation to bring the state into compliance with the national ID law."

mandate coming into effect on July 1, 2009.[217] When it kicked in, the state imposed a mandate on public and private employers with more than 100 employees, going so far as to issue employment licenses to private employers and requiring verification of new hires as a condition for maintaining the license. The mandate kicked in for smaller private employers a year later. From that date on, all employers in South Carolina and all new employees were effectively required to turn over their private information and identification to the government for the privilege of running a business or earning a salary. It hardly comports with the state constitution's high-minded language.

South Carolina was stoutly resistant to REAL ID for a long time. However, the state still implemented several of the federal act's benchmarks and was integrating a new facial recognition system into its DMV's licensing process. Finally, in April 2017 South Carolina adopted legislation to bring the state into compliance with the national ID law.[218]

To make matters worse, South Carolina has signed an MOU with the FBI to join the NGI.[219] Although the memorandum is not yet public, similar agreements with other states and the Bureau's sample memorandum would point to South Carolina's agreement being largely similar to others; the state's criminal photo database and its license database will be integrated into the FBI's own system. Millions of law-abiding South Carolinians will have their pictures available for the FBI's perusal.

Law-enforcement officials in South Carolina can and do use license plate reader technology. The state police supervisory agency, the South Carolina Law Enforcement Division, operates an integrated plate reader system that allows participating local enforcement to "compare scanned numbers against stolen license plate information." This system, dubbed NCICEXT, draws from the integrated federal National Crime Information Center.[220]

South Dakota

South Dakota's record is mixed. The state is compliant with DHS's REAL ID benchmarks. The state legislature embraced the federal law's onerous requirements in 2009, after having passed a strongly worded anti–REAL ID resolution only a year earlier. DHS deemed the state compliant in 2012. Conversely, South Dakota does not impose an E-Verify mandate on employers, and voluntary uptake of the federal verification system has been relatively low (hovering around 1.5 percent of registered businesses in the state in 2011).[221]

At the same time South Dakota embraced REAL ID, it embraced facial recognition. The state's adoption of the technology was quiet—so quiet that most members of the state legislature were not even aware of the state DMV's $600,000 purchase and installation of the necessary hardware and software.[222] Nor were they aware that access to the database can be granted to state law enforcement without a warrant. All officers need, according to the program's manager, is to be involved in an active investigation and make a request to the manager's office.[223] The lack of legislative oversight and judicial process is troubling, to say the least.

Finally, South Dakota does have license plate readers—but only in small Aberdeen. Installed on two of the town's eight police cars, it was paid for by a $38,000 DHS grant. The money gave the town the dubious distinction of being the only one to use it in the Mount Rushmore State.[224]

Tennessee

The Volunteer State's record is poor on privacy and ID issues. Tennessee is compliant with REAL ID, according to DHS's current standards, despite some early opposition in the legislature.[225] Driver information—including facial scans, biometric data, and other physical markers—is considered protected information under state law, with penalties for disclosure or illicit access to systems containing the information.[226] However, the state allows for disclosures of the information to police and other law-enforcement officials conducting "any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court

or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state or local court."[227] Information is also allowed to be disclosed to insurers, researchers, marketers, and other private individuals or groups, provided they can prove a need and promise not to disclose information without the subject's consent.[228] In short, the protections are loose.

Additionally, Tennessee was an eager adopter of an E-Verify mandate, with Gov. Bill Haslam (R) signing the Lawful Employment Act in 2011.[229] The law largely mirrors South Carolina's staged implementation of a mandate, ordering private businesses of decreasing size to use the system by certain dates. Only employers with fewer than five employees are exempt. Tennessee's law broadly resembles proposals floated by certain federal politicians for national mandatory E-Verify, such as in the 2013 Senate omnibus immigration bill.[230]

Finally, Tennessee's police forces have been eager adopters of license plate readers. The Tennessee Highway Patrol operates at least 48 mounted devices statewide, all paid for in part by a grant from the federal government.[231] Large municipalities such as Clarksville, Jackson, and Nashville all have local police forces that operate plate readers; Murfreesboro and Knoxville do not.[232] Of course, since the Highway Patrol operates statewide, all Tennesseans face the risk of having their locations and movements tracked by the state.

Texas

Texas's sheer size in both geography and population means that the state (like California and New York) plays an outsized role in national debates. All in all, when it comes to privacy, the Lone Star State's record is mixed, with some strengths and weaknesses.

In December 2014, then-governor Rick Perry (R) issued Executive Order RP-80, which requires all state agencies and contractors engaged in projects with state agencies to use E-Verify.[233] In 2015, SB 374 put the E-Verify requirement into statute and expanded it to include public higher-education institutions.[234]

Texas began complying with DHS's requirements under the REAL ID Act in 2016, and even before that the state had adopted many of DHS's compliance benchmarks.[235] Those benchmarks include biometrics collection and, at the DMV, a facial recognition system. Most prominently, as part of issuing new licenses or renewing old ones, the state now demands that Texans get fingerprinted, and their license photos join millions of others that are in the state's facial image database.[236] Both the fingerprint and facial-imaging database can be accessed by police to stop fraud, terrorism, or illegal immigration or for a host of other reasons.[237] Although searches are supposed to be targeted, 250 Department of Public Safety officials (including some members of law enforcement) can access the system at will; others must request a search.[238]

Finally, Texas has little in the way of curbs on the use of license plate readers. Indeed, jurisdictions in the state have been eager adopters of the technology.[239] Jurisdictions ranging from Austin and the sprawl of Dallas–Fort Worth to Highland and Grapevine have purchased systems, often using funds from the federal government with little state oversight or direction. The lack of oversight cannot be stressed enough: Grapevine (population 48,447 in 2012) uses multiple cameras and, according to the Grapevine Police Department, imposes no time limits on data retention—nor does it control access to the database, allowing any officer in the database.[240] In a town of fewer than 50,000 people, police had nearly two million plate captures in their database as of August 2012, and the system performed nearly 16,000 captures a day.[241] The numbers raise serious concerns about the scope of these systems and programs as they go state- and nationwide.

Utah

Utah's record is similarly mixed on privacy and ID issues. The Beehive State is REAL ID compliant, despite having a ban on compliance

"Texas began complying with the U.S. Department of Homeland Security's requirements under the REAL ID Act in 2016."

> "The Beehive State is REAL ID compliant, despite having a ban on compliance on the statute books."

on the statute books.[242] Utah's own, state-based licensing standards are as strict as those set out by the REAL ID Act, and DHS considers Utah licenses to meet federal standards. It is, essentially, a pantomime, with Utah enacting REAL ID by another name.[243] On E-Verify, at least, the state is direct in its adoption of the federal program: all public-sector entities and all private-sector entities with greater than 15 employees must use the verification system.[244]

Part of Utah's REAL-ID-but-not-REAL-ID dance is the use of biometric and facial recognition software. Access is limited to a dozen state Department of Public Safety employees and three licensing bureau officials, while other law-enforcement officers must provide requests.[245] Although the technology's use is largely limited to multiple-license fraud investigations, some commentators have noted its potential for expansion and becoming mobile. More widespread use will be debated, but at least one commentator, writing in the Utah Bar Association's journal, believes that usage would require a warrant under state law.[246]

Finally, Utah has limited the use of license plate readers. Use prior to 2012 was largely unrestrained by state statute. That changed with 2013's successful SB196, which created hard time limits for how long plate captures could be stored (9 months for law enforcement and 30 days for authorized private entities). It also lays out when the readers can and cannot be used, prevents disclosure, and classifies plate and location information as private information under state law.[247] Although Utah needs to work on its REAL ID and E-Verify problems, the state's plate capture law could serve as a useful model for other states.

Vermont

Unlike neighboring, libertarian-leaning New Hampshire, Vermont has a decidedly mixed record when it comes to the protection of privacy and ID rights. Although Vermont has rejected an E-Verify mandate for public and private employers, the Green Mountain State was an early adopter of the federal national ID law. The state began issuing compliant IDs on January 1, 2014.

Even prior to the adoption of REAL ID, Vermont's issuance of (optional) enhanced driver's licenses (valid for cross-border travel with Canada and Mexico) necessitated the establishment of a facial recognition system.[248] The state claims the use of the technology is to fight fraud and multiple license issuance. The state DMV does strictly control access to the image database. No law-enforcement agency has direct access to the system, and only select employees have access within the DMV. Law enforcement is required to make requests to the DMV if officials need facial images as part of an investigation.[249]

In a similar vein, Vermont has restricted the use of and access to license plate readers. Although police in the state can use the devices if necessary, the legislature put in place requirements for use. Officers must be trained in the use of the technology, and they can access system data only if they are conducting an active investigation. A request must be made to a superior for access, and periodic reviews must be carried out to ensure that proper procedures are being followed.[250]

Virginia

The Old Dominion had one of the better records on privacy and ID rights until it recently abandoned resistance to REAL ID. Virginia has a partial E-Verify mandate. It applies only to new public-sector hires; it does not apply to private-sector employers or government contractors. The 2009 state legislative session's HB 1587 blocked participation in REAL ID so long as participation threatens to "compromise the economic privacy or biometric data of any resident of the Commonwealth."[251] But early last year the Virginia Department of Motor Vehicles began "scrambling" to implement the national ID mandate.[252]

Virginia does not use facial recognition technology as part of its licensing process, making it one of the few states not to use the technology.[253] In addition, the state's licenses are currently issued in greyscale, negating one

of the biometric markers (skin tone) commonly used by facial recognition systems. However, licensing authorities have considered implementing the technology in the future, and the state's infamous no-smiling policy is designed to ease a potential implementation.[254]

Virginia's biggest ID problem does not involve driver's licenses, but rather license plates. Police forces across the state use license plate readers; formerly, there was little to no check on access or limits on the length of time data may be stored. A 2012 opinion by then-attorney general Ken Cuccinelli declared that keeping a capture for more than 24 hours if it was not tied to an active investigation was most likely illegal.[255] This prompted some police forces to begin dumping data; others, mostly in the Washington, D.C., suburbs of Northern Virginia, have continued to retain the data.[256] A March 2015 bill in the Virginia legislature to impose further limits on the use of the technology passed both chambers, only to be amended by Gov. Terry McAullife (D). Unfortunately, that was not the end of the fight. After a subsequent showdown with the legislature over the scope of the limits on readers, the governor—on the losing end of a fight to widen the use of the technology—vetoed the legislation. Rather than reaching a compromise that would have protected Virginians' liberties, he let the perfect be the enemy of the good and stopped the entire bill.[257]

Washington

Washington was, until recently, one of the leaders on privacy and ID issues. The state was firmly noncompliant with REAL ID (having banned compliance in 2007's SB 5087), and it does not impose an E-Verify mandate on its citizens and employers.[258] But last year, Governor Jay Inslee (D) signed legislation to bring Washington into compliance with the national ID program.[259]

The state's DMV does operate a facial recognition system that is used for licensing but, unlike many states, Washington statutorily lays out what the system can be used for and who can use it. Strictly speaking, only select DMV personnel can access the system—according to Washington's code—and law enforcement cannot. The only time law enforcement is allowed access is when assisting the DMV in an investigation into license fraud. Otherwise, there is no access allowed.[260]

Washington's sole blemish on an otherwise spotless record is the state's handling of license plate readers. The devices are not restricted under state law. Vehicle registration information (like driver's license information) is considered private, protected information under state law—but no such protection exists for license plate or GPS data.[261] Although the systems are not used by municipalities in the state, they are used by state police forces, most prominently in Seattle. Washington should follow its own example on facial recognition restrictions and apply the same level of scrutiny to license plate readers.

West Virginia

West Virginia is no Washington. Although West Virginia does not have in place an E-Verify mandate, the state has adopted REAL ID standards and is compliant with current DHS standards under the federal law and all their liberty-trampling requirements.[262] Worse, West Virginia was one of the first adopters of then-primitive facial recognition software back in 2002. The question of the use of and access to the present system is murky, at best, with nothing in the state's laws regulating the system.[263]

Additionally, while not currently engaged in an MOU with the FBI on the Bureau's NGI program, the state is home to the Biometric Center of Excellence, the federal agency's central testing center for biometric data.[264] All these programs, combined with the use of license plate readers by state police and local forces large and small, underscore a worrisome truth: Mountaineers may always be free, but their state's practices threaten residents' privacy.

Wisconsin

Wisconsin's record is mixed. The state adopted REAL ID standards readily, issuing

"Washington was, until recently, one of the leaders on privacy and ID issues."

"Wyoming has a strong libertarian tradition, but the state's record is mixed on privacy and ID."

its first licenses satisfactorily for DHS in early 2013. At the same time, the state has—so far—declined to put in place an E-Verify mandate, but it has decided to participate in the attached RIDE program.[265]

Along with REAL ID standards and stricter driver's license policies, the state implemented a facial recognition system in 2005. As early as May 2006, state officials were touting how useful the technology was in cracking down on fraud and how the DMV could run daily thousands of pictures of innocent citizens through a database of more than 6 million images.[266] State law does prohibit free law-enforcement access to the database; all requests must be for active investigations, and all must pass through an official at the DMV.[267] It's all for the greater good, Wisconsinites are told—and they should consider themselves lucky, according to one state senator, since they're still allowed to smile in their scanned pictures.[268]

Wyoming

Wyoming has a strong libertarian tradition, but the state's record is mixed on privacy and ID. Wyoming is one of the states that is fully compliant with the federal REAL ID Act, probably the greatest blemish on the state's otherwise good record. It has been considered compliant since December 2012. Wyoming does not, however, impose an E-Verify mandate, preferring to leave the issue of use of the verification system up to the choice of public and private employers. The state does, however, participate in the E-Verify RIDE program.[269]

Despite the state's embrace of REAL ID, Wyoming is the only compliant state to not have or use a facial recognition system. According to a report from Gannett News Service, one Wyoming DMV official contacted for information on the state's policies was unaware that such technology even exists.[270] That anecdote raises other concerns, but Wyoming's legislators have an opportunity to capitalize on the situation and put a ban in place before the state's driving bureaucrats realize the technology exists.

Finally, according to Freedom of Information Act results obtained by Wyoming's branch of the ACLU, no police force or state government entity in the state currently operates license plate readers.[271] The police force in Casper purchased one camera in June 2009, but found the camera and system so inefficient that the whole package was returned to the vendor in early 2010.[272]

NOTES

1. Jim Harper, "REAL ID: A State-by-State Update," Cato Institute Policy Analysis no. 749, May 12, 2014.

2. Ibid.

3. Alex Nowrasteh, "E-Verify Does Not 'Turn Off' Job Magnet," *Cato at Liberty* (blog), March 11, 2014, http://www.cato.org/blog/e-verify-does-not-turn-job-magnet.

4. Jim Harper, "E-Verify Wrong for America," *The Hill*, May 23, 2013, http://www.cato.org/publications/commentary/e-verify-wrong-america.

5. Alex Nowrasteh, "The Economic Costs of E-Verify," *The Federalist*, November 11, 2013, http://www.cato.org/publications/commentary/economic-costs-e-verify; and Jim Harper, "Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration," Cato Institute Policy Analysis no. 612, March 6, 2008, http://www.cato.org/publications/policy-analysis/electronic-employment-eligibility-verification-franz-kafkas-solution-illegal-immigration.

6. Jim Harper, "Idaho Cooperates with Homeland Security on National ID," *Cato at Liberty* (blog), July 19, 2013, http://www.cato.org/blog/idaho-cooperates-homeland-security-national-id.

7. Jim Harper, "Congress Pushes Biometrics," *Cato at Liberty* (blog), January 5, 2012, http://www.cato.org/blog/congress-pushes-biometrics.

8. Anthony Cotton, "Increasing Police Use of License-Plate Scanner Technology Raises Privacy Concerns," *Denver Post*, May 26, 2015, http://www.denverpost.com/2015/05/26/increasing-police-use-of-license-plate-scanner-technology-raises-privacy-concerns/.

9. FBI National Press Office, "FBI Announces Contract Award for Next Generation Identification System," Federal Bureau of Investigation, February 12, 2008, https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-contract-award-for-next-generation-identification-system.

10. Brian Shockley, "Alabama Criminal Justice Information Center Leverages License Plate Recognition Analytics and Data from Vigilant Solutions (Press release)," Vigilant Solutions, Inc., April 25, 2014, http://vigilantsolutions.com/press/acjic-implements-vigilant-license-plate-reader-analytics-data.

11. Brian Heaton, "Facial ID Tech Being Tested at Alabama County Jail," *Government Technology,* April 18, 2012, http://www.govtech.com/public-safety/Facial-ID-Tech-Tested-Alabama-County-Jail.html.

12. Ibid.; and Larry Amerson, Sheriff, Anniston, Calhoun County, Alabama, on Behalf of the National Sheriffs' Association, Statement for the Record, Hearing of the Subcommittee on Privacy, Technology and the Law of the Committee on the Judiciary of the United States Senate, July 18, 2012 (Serial No. J-112-87).

13. Ala. Code § 13A.11.30 (2014).

14. Ala. Const. art. I, §22.

15. Erwin Chemerinsky, "Privacy and the Alaska Constitution: Failing to Fulfill the Promise," *Alaska Law Review* 20: 29 (2003).

16. *Roberts v. State of Alaska,* 445 P.2d 674 (Alaska 1968).

17. P. 2d 494 (Alaska 1975).

18. Alaska Statutes § 44.41.035 (2015).

19. Rena Delbridge, "Facial Recognition and Fingerprint Scans?" *Alaska Dispatch News*, March 2, 2010, http://www.adn.com/article/facial-recognition-and-fingerprint-scans.

20. "State of Alaska D.M.V: WEI and Software AG Help the State Save Money and Increase Security with In-House Digital Driver License Management System," WEI, Inc., and Software AG, Inc., http://www.weiinc.com/Documents/AlaskaCaseStudy.pdf.

21. Office of the Governor, "Governor Walker Signs Legislation to Make Alaska Real I.D.-Compliant," May 19, 2017, https://gov.alaska.gov/newsroom/2017/05/governor-walker-signs-legislation-to-make-alaska-real-i-d-compliant/.

22. Ariz. Const., art. II, §8.

23. Griselda Nevarez, "Arizona Rolls Out REAL ID–Compliant Licenses and IDs Today," *Phoenix New Times*, April 1, 2016, http://www.phoenixnewtimes.com/news/arizona-rolls-out-real-id-compliant-licenses-and-ids-today-8184300.

24. Ariz. Rev. Statutes §23-211 to 216.

25. See, for example, Chamber of Commerce of *U.S. v. Whiting*, 131 S. Ct. 1968 (2011).

26. "Arizona Finds Success with Automated License Plate Readers," *Government Product News*, November 6, 2006, http://americancityandcounty.com/issue20060101/arizona-finds-success-automated-license-plate-readers.

27. Ariz. Rev. Statutes §13-2412.

28. Philip A. Elmore, "'That's Just Pillow Talk, Baby': Spousal Privileges and the Right to Privacy in Arkansas," *Arkansas Law Review* 67:961 (2014).

29. HB 1573, 2015 Reg. Sess. (AR 2015).

30. Act 1491, 2013 Reg. Sess. (AR 2013).

31. Cyrus Farivar, "Private Firms Sue Arkansas for Right to Collect License Plate Reader Data," *Ars Technica*, June 11, 2014, http://arstechnica.com/tech-policy/2014/06/private-firms-sue-arkansas-for-right-to-collect-license-plate-reader-data.

32. *Digital Recognition Network, Inc. et al. v. Beebe et al.*, http://www.scribd.com/doc/229019743/DRN-and-Vigilant-v-Beebe-and-McDaniel-Complaint.

33. "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field," the International Justice and Public Safety Network,

June 30, 2011, https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf.

34. Calif. Const., art. I, §1.

35. J. Clark Kelso, "California's Constitutional Right to Privacy," *Pepperdine Law Review* 19, no. 2 (1992): 328–29, http://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1631&context=plr.

36. Ibid.

37. Associated Press, "California Could Spend 220M to Upgrade Drivers Licenses," May 15, 2017, https://www.usnews.com/news/best-states/california/articles/2017-05-13/california-could-spend-220m-to-upgrade-drivers-licenses.

38. California Labor Code, Div. 3, Ch. 2, §2.5.

39. Jon Campbell, "License Plate Recognition Logs Our Lives, Long before We Sin," *LA Weekly*, June 21, 2012, http://www.laweekly.com/2012-06-21/news/license-plate-recognition-tracks-los-angeles.

40. "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field."

41. "Police Cameras Track Millions of License Plates, Compile Databases," *Denver Post*, July 18, 2013, http://www.denverpost.com/ci_23682448/police-cameras-track-millions-license-plates-compile-databases.

42. Harper, "REAL ID: A State-by-State Update."

43. Ken Dixon, "The Buried Lede: Connecticut ACLU This Afternoon, in Opposition to License-Plate Scanners, Will Allege That We Live in a Free Society," *Connecticut Post*, March 4, 2014, http://blog.ctnews.com/dixon/2014/03/04/the-buried-lede-connecticut-aclu-this-afternoon-in-opposition-to-license-plate-scanners-will-allege-that-we-live-in-a-free-society.

44. Ibid.; Connecticut General Assembly, "Automatic License Plate Recognition Systems," Office of Legislative Research Report 2012-R-0482, http://www.cga.ct.gov/2012/rpt/2012-R-0482.htm.

45. Corey McKenna, "Delaware to Use Facial Recognition in Issuing Drivers' Licenses," *Government Technology*, April 17, 2009, http://www.govtech.com/public-safety/Delaware-to-Use-Facial-Recognition-in.html.

46. Del. Code Ann., Tit. 11, §§1902(a), 1321(6) (2003).

47. Fla. Const., Article I, §12.

48. Fla. Const., Article I, §23.

49. Fla. Stat. §23.322 (2015).

50. Fla. Exec. Order No. 11-02 (January 4, 2011); and Fla. Exec. Order No. 11-116 (May 27, 2011).

51. Sheppard Mullin Richter & Hampton, LLP, "E-Verify on the Fritz Likely Due to Florida Going Live on the RIDE Program," December 12, 2012, http://www.jdsupra.com/legalnews/e-verify-on-the-fritz-likely-due-to-flor-38559.

52. "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field."

53. "About the Biometric Center of Excellence," Federal Bureau of Investigation, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/about/about-the-biometric-center-of-excellence.

54. "FY2015 Authorization and Budget Request to Congress," Federal Bureau of Investigation, March 2014, http://www.justice.gov/sites/default/files/jmd/legacy/2013/10/03/fbi-justification.pdf.

55. Brett Clarkson, "Your License Plate is Posing for Pictures—and You Probably Don't Even Know It," *Sun Sentinel* (Florida), August 3, 2013, http://articles.sun-sentinel.com/2013-08-03/news/fl-palm-license-plate-cameras-20130803_1_plate-data-license-plate-cameras.

56. Gil Aergerter, "License Plate Data Not Just for Cops: Private Companies Are Tracking Your Car," NBC News, July 19, 2013, http://www.nbcnews.com/news/other/license-plate-data-not-just-cops-private-companies-are-tracking-f6C10684677.

57. Jim Harper, "The End of the License Plate," *Washington Examiner*, April 18, 2015, http://www.washingtonexaminer.com/the-end-of-the-license-plate/article/2563177.

58. Sarah Freishtat, "Just a Face in a Crowd? Scans Pick Up ID,

Personal Data," *Washington Times*, July 26, 2012, http://www.washingtontimes.com/news/2012/jul/26/just-a-face-in-a-crowd-scans-pick-up-id-personal-d.

59. Ga. Code §40-5-2, §50-18-72.

60. Georgia House Bill 87 (Reg. Sess., 2011-2012).

61. Rhonda Cook, "Are Automatic License Plate Readers a Violation of Privacy?" *Atlanta-Journal Constitution*, November 30, 2012, http://www.ajc.com/news/news/are-automatic-license-plate-readers-a-violation-of/nTKg7.

62. Keith Farner, "Ga. Supreme Court Upholds Ruling in License Plate Reader Case," *Gwinnett Daily Post* (Lawrenceville, GA), July 6, 2014, http://www.gwinnettdailypost.com/news/2014/jun/30/ga-supreme-court-upholds-ruling-in-license-plate.

63. Hawaii Const. Article I, §6 and §7.

64. "EFF Sues FBI for Access to Facial-Recognition Records," Electronic Frontier Foundation, June 26, 2013, https://www.eff.org/press/releases/eff-sues-fbi-access-facial-recognition-records; and "Memorandum of Understanding Between the Federal Bureau of Investigation and the State of Hawaii Department of the Attorney General for the Interstate Facial Recognition System," November 2011, https://www.eff.org/files/filenode/hawaii_mou_ngi_face-recognition.pdf.

65. Ibid.

66. "FBI Facial Recognition Documents Complaint," Electronic Frontier Foundation, June 26, 2013, https://www.eff.org/node/74758.

67. Brent Remanda, "HPD Says License Plate Scanners Are Working," KHON-TV 2, February 25, 2015, http://khon2.com/2015/02/25/hpd-reports-license-plate-scanners-work.

68. Id. HB 606, (2d Reg. Sess., 2008).

69. Associated Press, "Idaho Gov. C. L. 'Butch' Otter approves Real ID legislation," April 3, 2016, http://idahostatejournal.com/members/idaho-gov-c-l-butch-otter-approves-real-id-legislation/article_ffc62f09-a15b-533e-b1c8-d7296be591ff.html.

70. Austin Hill, "License Plate Data Scanned, Stored in Three Idaho Cities," Idaho Freedom Foundation, July 20, 2013, http://idahofreedom.org/license-plate-data-scanned-stored-in-three-idaho-cities/; see, more generally, the Idaho Code.

71. Id. Exec. Order No. 2009-10 (May 29, 2009).

72. Harper, "Idaho Cooperates with Homeland Security on National ID."

73. Ill. Const. Article I, §6, §12.

74. Doug Finke, "Illinois Seeking One More REAL ID Extension," September 2, 2017, http://www.sj-r.com/news/20170902/illinois-seeking-one-more-real-id-extension.

75. Ill. Public Act 095-0138.

76. Eric D. Ledbetter and Grant Sovern, "New Illinois E-Verify Law Takes Effect on January 1, 2010: Special Illinois Procedures Required," Quarles & Brady, LLP, Labor and Employment Law Update, December 18, 2009, https://www.quarles.com/eric-d-ledbetter/publications-presentations/new-illinois-e-verify-law-takes-effect-on-january-1-2010-special-illinois-procedures-required/.

77. Chandler Harris, "Biometrics Stems Driver's License Fraud," *Government Technology*, June 25, 2008, http://www.govtech.com/pcio/Biometrics-Stems-Drivers-License-Fraud.html.

78. Matt Stroud, "Did Chicago's Facial Recognition System Catch Its First Crook?" *The Verge*, August 8, 2014, http://www.theverge.com/2014/8/8/5982727/face-wreck-how-advanced-tech-comes-up-short-for-police.

79. Ibid; and "Chicago's Video Surveillance Cameras: A Pervasive and Unregulated Threat to Our Privacy," American Civil Liberties Union of Illinois, February 2012, http://www.aclu-il.org/wp-content/uploads/2012/06/Surveillance-Camera-Report1.pdf.

80. American Civil Liberties Union, "You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements," American Civil Liberties Union of New York, July 2013, https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.

81. Sandra Chapman, "Indiana BMV Gets Top Honors," *WTHR 13*, September 27, 2010, http://www.wthr.com/story/13225281/indiana-bmv-gets-top-honors.

82. Indiana Senate Enrolled Act 509 (1st. Reg. Sess., 2011).

83. Jaikumar Vijayan, "Wipe That Smile off Your Face, Indiana BMV Tells Drivers," *Computer World*, December 10, 2008, http://blogs.computerworld.com/wipe_that_smile_off_your_face_indiana_bmv_tells_drivers.

84. "Indiana Gaming Commission Uses Facial Recognition to Nab Robber," *Fox 19 WXIX*, December 17, 2012, http://www.fox19.com/story/20359024/falmouth-robbery-suspect-traced-to-lawrenceburg-casino-arrested.

85. Christian Scheckler, "South Bend Police Adopt License Plate Reader Policy," *South Bend Tribune*, April 17, 2014, http://www.southbendtribune.com/news/crime/police-adopt-license-plate-reader-policy/article_8796ec64-c617-11e3-b355-0017a43b2370.html.

86. Ibid.

87. Ind. SB 417 (1st. Reg. Sess., 2014).

88. REAL ID web page, Iowa Department of Transportation, http://www.iowadot.gov/mvd/realid/home.html.

89. "Facial Recognition Nabs Fugitive after 41 Years on Run," *Newsmax*, June 26, 2014, http://www.newsmax.com/SciTech/fugitive-Carnes-facial-recognition/2014/06/26/id/579503.

90. Mike Wiser, "Program Pushes Facial Recognition for Iowa Sex Offenders," *The Gazette* (Iowa), December 17, 2012, http://thegazette.com/2012/12/17/program-pushes-facial-recognition-for-iowa-sex-offenders.

91. "Iowa to Explore Facial Recognition Technology," *Waterloo-Cedar Falls Courier*, January 7, 2014, http://wcfcourier.com/news/local/crime-and-courts/iowa-to-explore-facial-recognition-technology/article_2d6e6896-7786-11e3-9491-0019bb2963f4.html.

92. "Kansas Lawmakers Nix E-Verify Immigration Enforcement Proposal," Fox News Latino, May 14, 2012, http://www.foxnews.com/politics/2012/05/14/kansas-lawmakers-negotiating-2013-budget-nix-immigration-enforcement-proposal.html.

93. Harper, "REAL ID: A State-by-State Update."

94. "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field."

95. "Automatic License Plate Reader FOIA Documents: Kansas," American Civil Liberties Union, https://www.aclu.org/files/FilesPDFs/ALPR/kansas/alprpra_hutchinsonpd_hutchinsonka.pdf.

96. Jack Brammer, "Bevin Signs Real ID Driver's License Bill," March 22, 2017, http://www.kentucky.com/news/local/education/article140176623.html.

97. "New Facial Recognition Software Fights Identity Fraud," *Techlines: Commonwealth of Kentucky Technology News*, April 1, 2005, http://techlines.ky.gov/2005/april/facial_recognition.htm.

98. J. D. Tuccille, "30,000 Cops Can Access Ohio's Facial Recognition Database without Oversight, Says Report," *Reason.com*, September 22, 2013, http://reason.com/blog/2013/09/23/30000-cops-can-access-ohios-facial-recog.

99. "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field."

100. La. Rev. Stats. §38-2212.10.

101. Kevin Litten, "Bobby Jindal Vetoes License Plate Scanner Legislation over Privacy Concerns," *Times–Picayune* (New Orleans), June 19, 2015, http://www.nola.com/politics/index.ssf/2015/06/bobby_jindal_vetoes_license_pl.html.

102. Office of the Governor, "Gov. Edwards Signs REAL ID into Law," June 14, 2016, http://gov.louisiana.gov/news/gov-edwards-signs-real-id-into-law.

103. Jim Harper, "State ID Databases Hacked," *Cato at Liberty* (blog), September 20, 2016, http://www.cato.org/blog/state-id-databases-hacked.

104. Harper, "REAL ID: A State-by-State Update"; and Steve Mistler, "Maine House Approves 'Real ID' Bill Allowing Individuals to Opt Out," *Bangor Daily News* (Bangor, ME), April 11, 2017, http://bangordailynews.com/2017/04/11/politics/maine-house-approves-real-id-bill-allowing-individuals-to-opt-out.

105. Kevin Miller, "Real ID Bill Passes, Headed to LePage's Desk for Signature," *Portland Press Herald* (Portland, ME), April 25, 2017, http://www.pressherald.com/2017/04/25/real-id-bill-passes-headed-to-lepages-desk-for-signature/.

106. Alex Nowrasteh and Jim Harper, "Checking E-Verify:

The Costs and Consequences of a National Worker Screening Mandate," Cato Institute Policy Analysis no. 775, July 7, 2015, pg. 3.

107. Tuccille, "30,000 Cops Can Access Ohio's Facial Recognition Database without Oversight."

108. David Hench, "Smile, You Scofflaws, You're on County Camera," *Portland Press Herald*, August 1, 2012 http://www.pressherald.com/2012/08/01/smile-you-liars-youre-on-county-camera_2012-08-02/.

109. Maine Rev. Stats. §29-19-2117-A.

110. Ibid.

111. "Maryland Meets REAL ID Standards," Maryland Motor Vehicle Administration, December 21, 2012, http://www.mva.maryland.gov/about-mva/press-releases/2012/122112.htm. Non-federal licenses are an option under REAL ID—licenses that don't comply with federal mandates must have distinct features indicating that. When states offer them, that is a minor convenience for their residents, if not their privacy, but whether and how well the state promotes them makes an important difference.

112. Thomas Ahearn, "Three More States Join E-Verify RIDE Program Beginning July 31," Employment Screening Resources, August 21, 2017, http://www.esrcheck.com/wordpress/2017/08/-1/three-more-states-join-e-verify-ride-program-beginning-july-31/.

113. Md. Ann. Code §3-509 (2011 Replacement Volume and 2013 Supplement).

114. Memorandum of Understanding between the Federal Bureau of Investigation and the Maryland Department of Public Safety and Correctional Services, Information Technology and Communications Division, for the Interstate Photo System Facial Recognition Pilot, https://www.eff.org/document/maryland-memorandum-understanding-mou-fbi-face-recognition-photos.

115. "Massachusetts Senate to Governor Patrick: Comply with REAL ID," Coalition for a Secure Driver's License, March 6, 2013, http://www.prnewswire.com/news-releases/massachusetts-senate-to-governor-patrick-comply-with-real-id-195654251.html.

116. Robert Charette, "Here's Looking at You, and You, and You. . . ," *IEEE Spectrum*, July 25, 2011, http://spectrum.ieee.org/riskfactor/computing/it/heres-looking-at-you-and-you-and-you-.

117. Stephanie Ebbert, "New Tool for Police Is Good with Faces," *Boston Globe*, July 18, 2011, http://www.boston.com/news/local/massachusetts/articles/2011/07/18/device_allows_facial_recognition_data_to_be_tapped_remotely/?page=1.

118. Meaghan E. Irons, "Caught in a Dragnet," *Boston Globe*, July 17, 2011, http://www.boston.com/news/local/massachusetts/articles/2011/07/17/man_sues_registry_after_license_mistakenly_revoked.

119. Harper, "Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration."

120. Alison Bauter, "New Mass. IDs: What 'REAL ID' Means for You," *Beacon Hill Patch* (Beacon Hill, MA), July 26, 2016, https://patch.com/massachusetts/beaconhill/real-id-bill-becomes-law-heres-what-it-means-you.

121. Perry A. Farrell, "Michigan to Start Issuing New IDs That Will Be Accepted on Domestic Flights," *Detroit Free Press*, August 21, 2017 http://www.freep.com/story/news/local/michigan/2017/08/21/new-michigan-residenmichigan-residents-can-receive-new-compliant-drivers-licenses-starting-new-monda/587105001/.

122. Mich. HB 5365 (2012 Regular Session).

123. Siddhartha Mahanta, "Privacy Concerns Linger over FBI's New Facial Recognition System," *Huffington Post*, October 24, 2012, http://www.huffingtonpost.com/2012/10/24/fbi-facial-recognition_n_2009690.html.

124. Harper, "REAL ID: A State-by-State Update."

125. Erin Golden and Jennifer Brooks, "Dayton Signs Bill Conforming Minn. Driver's Licenses with Federal Standards," *Star Tribune* (Minneapolis, MN), May 18, 2017, http://www.startribune.com/compromise-on-real-id-licenses-headed-for-a-vote/422788024.

126. Minn. Stats. 2014, §16C.075.

127. Jen Brooks, "Dayton Vetoes E-Verify Bill," *Star Tribune* (Minneapolis, MN), April 24, 2012, http://www.startribune.com/dayton-vetoes-e-verify-bill/148716715.

128. "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field."

129. Minn. Stats. 2014, §171.07.

130. Eric Roper, "Driver's License Snooping Gets Costly for Taxpayers," *Star Tribune* (Minneapolis, MN), September 12, 2013, http://www.startribune.com/local/west/220066801.html.

131. Ibid.

132. Minn. Stats. 2014, §13.05.

133. Harper, "REAL ID: A State-by-State Update"; and Jason Hancock, "REAL ID Bill Runs into Roadblock in Missouri Senate," February 22, 2017, http://www.kansascity.com/news/politics-government/article134380404.html.

134. Miriam Jones, "Mississippi State Police Implement Facial Recognition Technology," *Government Technology*, August 7, 2003, http://www.govtech.com/security/Mississippi-State-Police-Implement-Facial-Recognition.html.

135. "Police in Jackson, MS, Use Genetec License Plate Recognition Technology," *Government Security News*, March 14, 2013, http://www.gsnmagazine.com/article/28730/police_jackson_ms_use_genetec_license_plate_recogn.

136. Harper, "REAL ID: A State-by-State Update."

137. Jason Hancock, "Greitens Signs Real ID Legislation, Putting Missouri in Compliance with Federal Law," *Kansas City Star*, June 12, 2017, http://www.kansascity.com/news/politics-government/article155700884.html.

138. Mo. Rev. Stats. §285.530.1.

139. "ID Facial Recognition Program Halted," *Columbia Tribune*, April 24, 2013, http://www.columbiatribune.com/news/id-facial-recognition-program-halted/article_e8217dd4-acfe-11e2-b645-10604b9f6eda.html.

140. Mo. HB 5 (1st Regular Session, 2011).

141. Const. Mont., Article II, §10.

142. MTN News, "Montana Complies with Federal REAL ID Law," KPAX, June 1, 2017, http://www.kpax.com/story/35565701/montana-complies-with-federal-real-id-law.

143. "Goals & Objectives," Montana Department of Justice, https://dojmt.gov/about/goals-objectives/.

144. Craig Timberg and Ellen Nakashima, "State Photo-ID Databases Become Troves for Police," *Washington Post*, June 17, 2013, http://www.edmondsun.com/local/x331658120/State-photo-ID-databases-become-troves-for-police?zc_p=4.

145. Brett Berntsen, "No Place to Hide," *Montana Journalism Review* (2014), http://mjr.jour.umt.edu/?p=2398.

146. Neb. Legislature Bill 261 (Regular Session, 2011).

147. "E-Verify Notice," Nebraska Department of Revenue, http://www.revenue.nebraska.gov/incentiv/e-verify_notice.html.

148. "Nebraska Town Hasn't Been Able to Enforce Immigration Rule," *Rapid City Journal*, July 10, 2014, http://rapidcityjournal.com/news/local/nebraska-town-hasn-t-been-able-to-enforce-immigration-rule/article_5adfc23c-089c-11e4-a8a0-0019bb2963f4.html.

149. "Nebraska Driver's License and ID Card Information," https://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/Nebraska_RIDE_Fact_Sheet.pdf.

150. "New System Helps Nebraska DMV Crack Down on Fraud, ID Theft," *Lincoln Journal Star*, September 11, 2009, http://journalstar.com/news/local/govt-and-politics/new-system-helps-nebraska-dmv-crack-down-on-fraud-id/article_5bd3b5b0-9f3b-11de-9240-001cc4c03286.html.

151. Neb. Rev. Stats. §60-484.02.

152. "Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field."

153. "Memorandum of Understanding between the Federal Bureau of Investigation Criminal Justice Information Services Division and the Nebraska Department of Motor Vehicles," https://www.epic.org/foia/fbi/faces/FBI-MOUs-FACES-Unit.pdf.

154. "Automatic License Plate Readers: A Threat to Americans' Privacy," American Civil Liberties Union of Nebraska, July 17, 2013, https://www.aclunebraska.org/en/automatic-license-plate-readers-a-threat-to-americans-privacy.

155. Harper, "REAL ID: A State-by-State Update."

156. Ibid.

157. "Secretary of State Ross Miller Says State Contractors Should Use Federal E-Verify Program to Check for Eligible Workers," Office of the Nevada Secretary of State, December 14, 2012, http://nvsos.gov/sos/Home/Components/News/News/555/309?npage=7&arch=1.

158. Sean Whaley, "Driving Cards Bring Jump in Potential Nevada DMV Fraud Cases," *Las Vegas Review-Journal*, January 17, 2014, https://www.reviewjournal.com/news/driving-cards-bring-jump-in-potential-nevada-dmv-fraud-cases/.

159. Mike Nyerges and Chrissie Thompson, "Does State Have Facial Recognition Software?" *Cincinnati Enquirer*, http://public.tableausoftware.com/views/FacialRecognition/Dashboard1?:showVizHome=no.

160. "Nevada Highway Patrol Using Automatic License Plate Recognition System for DEA," American Civil Liberties Union of Nevada, September 13, 2012, http://www.aclunv.org/press/nhp-using-alpr-system-dea.

161. Ibid.

162. N.H. HB 267 (Regular Session, 2015).

163. N.H. State Code §260:10-b.

164. N.H. State Code §651-F.

165. N.H. State Code §261:75-b.

166. N.H. State Code §236.

167. "New Hampshire Not Participating in Real ID," *Government Technology*, June 27, 2009, http://www.govtech.com/security/New-Hampshire-Not-Participating-in-Real.html.

168. New Hampshire Division of Motor Vehicles, "REAL ID," https://www.nh.gov/safety/divisions/dmv/driver-licensing/real-id/index.htm.

169. Alexi Friedman, "N.J. Driver's License Photos: Nothing to Smile About," *Star-Ledger*, September 21, 2012, http://www.nj.com/news/index.ssf/2012/09/drivers_license_photos_nothing.html; and David Matthau, "Will NJ Residents Be Able to Use Driver's Licenses as ID at Airports?", New Jersey 101.5, July 4, 2017, http://nj1015.com/will-nj-residents-be-able-to-use-drivers-licenses-as-id-at-airports/.

170. New Jersey Assembly Bill 1271 (2014 Regular Session).

171. "Attorney General and MVC Chief Showcase High-Tech Program 'Operation Facial Scrub' to Detect False Driver's Licenses," Office of the Attorney General of New Jersey, February 12, 2013, http://www.nj.gov/oag/newsreleases13/pr20130212a.html.

172. New Jersey Attorney General Directive no. 2010-5.

173. "Automatic License Plate Reader FOIA Documents: New Jersey," American Civil Liberties Union, https://www.aclu.org/technology-and-liberty/automatic-license-plate-reader-foia-documents-new-jersey.

174. Harper, "REAL ID: A State-by-State Update."

175. Nowrasteh and Harper, "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate," pg. 3.

176. "Memorandum of Understanding Between the Federal Bureau of Investigation Criminal Justice Information Services Division and the New Mexico Department of Motor Vehicles," https://www.epic.org/foia/fbi/faces/FBI-MOUs-FACES-Unit.pdf.

177. New York State Department of Motor Vehicles, "About Federal REAL ID," https://dmv.ny.gov/driver-license/about-federal-real-id.

178. "Governor Cuomo Announces 13,000 Identity Fraud Cases Investigated by DMV Using Facial Recognition Technology," Office of Governor Andrew M. Cuomo, March 5, 2013, https://www.governor.ny.gov/news/governor-cuomo-announces-13000-identity-fraud-cases-investigated-dmv-using-facial-recognition.

179. Rocco Parascandola, "NYPD Planning to Use Facial Recognition Technology to Match Mug Shots to Suspect Videos," *New York Daily News*, February 5, 2011, http://www.nydailynews.com/new-york/nypd-planning-facial-recognition-technology-match-mug-shots-suspect-videos-article-1.136071.

180. Matt Sledge, "NYPD License Plate Readers Will Be Able to Track Every Car Entering Manhattan," *Huffington Post*, March 13, 2013, http://www.huffingtonpost.com/2013/03/13/nypd-license-plate-readers_n_2869627.html.

181. Ibid.

182. Mike McAndrew, "NY Awards Police Agencies $550,270 to Buy Controversial License Plate Readers," *Syracuse.com,* April 15, 2014, http://www.syracuse.com/news/index.ssf/2014/04/ny_awards_police_agencies_550270_to_buy_license_plate_readers.html.

183. "NCDMV Continues Production of New Driver Licenses That Will Reduce Fraud, Better Integrate Technology," North Carolina Department of Motor Vehicles, January 9, 2014, https://apps.ncdot.gov/newsreleases/details.aspx?r=9209; and Richard Stradling, "N.C. to Offer REAL ID Cards Starting May 1," *Charlotte News-Observer*, April 26, 2017, http://www.newsobserver.com/news/politics-government/article146896864.html.

184. Nowrasteh and Harper, "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate," pg. 3.

185. N.C. HB 36 (2012 Regular Session); N.C. SB 1523 (2007 Regular Session).

186. "N.C. DMV to Use Facial Recognition Scanners," *Security-Info Watch*, September 30, 2004, http://www.securityinfowatch.com/news/10592107/nc-dmv-to-use-facial-recognition-scanners.

187. N.C. SB 623 (2013 Regular Session).

188. Dave Thompson, "'Real ID' to Be Rolled Out Next Spring (2018)," *Prairie Public News* (Fargo, ND), June 12, 2017, http://news.prairiepublic.org/post/real-id-be-rolled-out-next-spring-2018#stream/0.

189. Nowrasteh and Harper, "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate," pg. 3.

190. "North Dakota Driver's License and ID Card Information," U.S. Citizenship and Immigration Services, https://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/NorthDakota_RIDE-FactSheet.pdf.

191. Brian Gehring, "Facial Recognition Software Used by DOT," *Bismarck Tribune*, August 3, 2012, http://bismarcktribune.com/news/local/facial-recognition-software-used-by-dot/article_dd7d0f7e-dcde-11e1-a6a0-001a4bcf887a.html.

192. Cyrus Farivar, "Your Car, Tracked: The Rapid Rise of License Plate Readers," *Ars Technica*, September 27, 2012, http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers.

193. Randy Ludlow, "Ohio Pulls Plans to Comply with Federal ID Law," *Columbus Dispatch*, December 6, 2013, http://www.dispatch.com/content/stories/local/2013/12/06/state-pulls-plans-to-comply-with-federal-id-law.html.

194. Steve Stephens, "Real ID Rules Still on Hold, but Ohio in Compliance," *Columbus Dispatch*, November 26, 2015, http://www.dispatch.com/content/stories/local/2015/11/26/real-id-rules-still-on-hold-but-ohio-in-compliance.html.

195. Cornelius Frolik, "More Ohio Businesses Using Fed System to Verify Legal Status," *Dayton Daily News*, August 6, 2012, http://www.daytondailynews.com/news/news/more-ohio-businesses-using-fed-system-to-verify-le/nP92z/.

196. Tuccille, "30,000 Cops Can Access Ohio's Facial Recognition Database without Oversight."

197. Ibid.

198. Barbara Hoberock, "Oklahoma Now Has Real ID Law, but Don't Get in Line Yet for New Driver's License," *Tulsa World*, March 3, 2017, http://www.tulsaworld.com/homepagelatest/oklahoma-now-has-real-id-law-but-don-t-get/article_efb510c8-3816-58f5-a895-30c151a2ba25.html.

199. Ismael Estrada and Keith Oppenheim, "Oklahoma Targets Illegal Immigrants with Tough New Law," CNN, November 5, 2007, http://www.cnn.com/2007/US/11/02/oklahoma.immigration/.

200. "In a Law Suit, Okla. Woman Argues Biometric Driver's License Is 'a Sign of the Antichrist,'" *Homeland Security News Wire*, August 1, 2013, http://www.homelandsecuritynewswire.com/dr20130801-in-a-law-suit-okla-woman-argues-biometric-driver-s-license-is-a-sign-of-the-antichrist.

201. Jesse Wells, "OKC Police Purchase Controversial Crime-Fighting Tool," KFOR News Channel 4, December 4, 2012, http://kfor.com/2012/12/04/okc-police-purchase-controversial-crime-fighting-tool/.

202. "ACLU Seeks Details on Automatic License Plate Readers in Massive Nationwide Request," American Civil Liberties Union of Oklahoma, July 30, 2012, http://acluok.org/2012/07/aclu-

seeks-details-on-automatic-license-plate-readers-in-massive-nationwide-request.

203. Nowrasteh and Harper, "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate," pg. 3.

204. Elliot Njus, "Oregon Driver's License Holders Get Reprieve as State Moves toward Real ID Compliance," *Oregonian* (Portland, OR), July 10, 2017, http://www.oregonlive.com/commuting/index.ssf/2017/07/oregon_drivers_license_holders.html.

205. Ore. Rev. Stats. §801.063.

206. Kristian Voden-Fencil, "Portland Police Collect Thousands of License Plate Numbers," *WBUR-NPR*, December 12, 2013, http://hereandnow.wbur.org/2013/12/12/police-license-plate.

207. Harper, "REAL ID: A State-by-State Update."

208. Wallace McKelvey, "PennDOT: Real ID–Compliant Drivers Licenses Will Cost Pa. $30M+," Penn Live, August 29, 2017, http://www.pennlive.com/news/2017/08/real_id_licenses_pa_30_million.html.

209. Pa. SB 637 (2011 Reg. Sess.).

210. Sarah Rich, "Pennsylvania Facial Recognition Systems Integrate to Widen Search for Criminals," *Government Technology*, September 3, 2013, http://www.govtech.com/public-safety/Pennsylvania-Facial-Recognition-Systems-Integrate-to-Widen-Search-for-Criminals.html.

211. "Fulfilling Campaign Promise, Governor Lincoln D. Chafee Repeals Executive Order on E-Verify, Pledges More Tolerant, Welcoming Rhode Island," Press Office of the Office of the Governor of Rhode Island, January 5, 2011, http://www.ri.gov/press/view/12942.

212. Brian Crandall, "DMV Uses Biometrics to Fight Fraud, Crime," NBC 10 (Providence, RI), November 16, 2011, http://www.turnto10.com/story/21128278/dmv-uses-biometrics-to-fight-fraud-crime.

213. See DMV.org, "Identification Cards in Rhode Island," https://www.dmv.org/ri-rhode-island/id-cards.php.

214. R.I. HB 5150 (2013 Regular Session); R.I. SB 46 (2013 Regular Session).

215. R.I. Gen. Laws. § 31-10-26 (2012).

216. Const. of S.C., art. 1, §10.

217. Nowrasteh and Harper, "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate."

218. Andy Shain, "South Carolina Rolling Out New Driver's Licenses to Meet Government's REAL ID Rules," *Post and Courier*, May 1, 2017, http://www.postandcourier.com/news/south-carolina-rolling-out-new-driver-s-licenses-to-meet/article_1e27e532-2e95-11e7-9334-cfb0fa71b8df.html.

219. "Memorandum of Understanding Between the Federal Bureau of Investigation Criminal Justice Information Services Division and the South Carolina Department of Motor Vehicles," https://www.epic.org/foia/fbi/faces/FBI-MOUs-FACES-Unit.pdf.

220. "South Carolina Law Enforcement Division License Plate Reader File Access," South Carolina Law Enforcement Division, http://www.sled.sc.gov/Documents/CJIS/LPRFileAccess.pdf.

221. Marc Rosenblum and Lang Hoyt, "The Basics of E-Verify, the U.S. Employer Verification System," July 13, 2011, *Migration Information Source*, Migration Policy Institute, http://www.migrationpolicy.org/article/basics-e-verify-us-employer-verification-system.

222. Joe O'Sullivan, "State Conducting Facial Recognition Searches on Driver's License Photos," *Rapid City Journal*, July 21, 2013, http://rapidcityjournal.com/news/state-conducting-facial-recognition-searches-on-drivers-license-photos/article_aeef2950-900a-5d17-bb3a-90fe88609f13.html.

223. Ibid.

224. Elisa Sand, "Officers Capture License Plate Information," *Aberdeen News* (South Dakota), February 27, 2014, http://www.aberdeennews.com/news/local/officers-capture-license-plate-information/article_a8b451c4-4945-5568-91ab-8d5d4658d0ae.html.

225. Tennessee Senate Joint Resolution 248, (105th Gen. Assem. Reg. Sess. 2007); Tenn. SB 1934 (106th Gen. Assem. Reg. Sess. 2009); Tenn. HB 1426 (106th Gen. Assem. Reg. Sess. 2009).

226. Tenn. Code Ann. § 55-25-107.

227. Ibid.

228. Ibid.

229. Nowrasteh and Harper, "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate," pg. 3.

230. Border Security, Economic Opportunity, and Immigration Modernization Act of 2013, S.744, 113th Congress (2013–2014).

231. "Public Records Act Request, Received August 2, 2012," Department of Safety and Homeland Security (Tennessee), August 23, 2012, https://www.aclu.org/files/FilesPDFs/ALPR/tennessee/alprpra_departmentofsafetyandhomelandsecurity_nashvilletn_1.pdf; and Becky Campbell, "Local Police Not Part of U.S. License Plate Database Trend," *Johnson City Press* (Johnson City, TN), July 20, 2013, http://www.johnsoncitypress.com/law-enforcement/2013/07/20/Local-police-not-part-of-U-S-license-plate-database-trend.

232. "Automatic License Plate Reader FOIA Documents: Tennessee," American Civil Liberties Union, https://www.aclu.org/technology-and-liberty/automatic-license-plate-reader-foia-documents-tennessee.

233. Texas Executive Order No. RP-80.

234. Tex. Gov. Code §6.673.

235. Texas Department of Public Safety, "DPS Submits Plan for Federal Real ID Act," https://www.dps.texas.gov/DriverLicense/federalRealIdAct.htm.

236. Tim Cushing, "Texas Dept. of Public Safety Quietly Starts Demanding Full Set of Prints from Driver's License Applicants," *TechDirt*, July 24, 2014, https://www.techdirt.com/articles/20140721/09452027954/texas-dept-public-safety-quietly-starts-demanding-full-set-prints-drivers-license-applicants.shtml.

237. Dave Lieber, "Watchdog: Driver's License Centers Snatch Your Fingerprints," *Dallas Morning News*, June 19, 2014, http://www.dallasnews.com/investigations/watchdog/20140607-watchdog-drivers-license-centers-snatch-your-fingerprints.ece.

238. Mike Nyerges and Chrissie Thompson, "Does State Have Facial Recognition Software?" *Cincinnati Enquirer*, http://public.tableausoftware.com/views/FacialRecognition/Dashboard1?:showVizHome=no.

239. Forrest Wilder, "The Eyes of Texas Cops Are upon You," *Texas Observer* (Austin), July 15, 2010, http://www.texasobserver.org/the-eyes-of-texas-cops-are-upon-you/; and "Automatic License Plate Reader FOIA Documents: Texas," American Civil Liberties Union, https://www.aclu.org/technology-and-liberty/automatic-license-plate-reader-foia-documents-texas.

240. Capt. Mark R. Bills, "Public Records Request/Automatic License Plate Readers," Grapevine Police Department Office of Records, September 10, 2012, https://www.aclu.org/files/FilesPDFs/ALPR/texas/alprpra_grapevinePD_grapevineTX(6).pdf.

241. Ibid.

242. Utah Code §53-3-104.5

243. Harper, "REAL ID: A State-by-State Update."

244. Utah Code §13-47.

245. Nyerges and Thompson, "Does State Have Facial Recognition Software?

246. Adam Alba, "In Utah, Scanning a Person's Face or Iris to Determine Identity Is a Search Justified Only in Limited Circumstances," *Utah State Bar Journal Online*, November 7, 2011, http://silk.utahbar.org/utah-bar-journal/article/in-utah-scanning-a-persons-face-or-iris-to-determine-identity-is-a-search-justified-only-in-limited-circumstances/.

247. Utah Code §41-6a-2001.

248. "Facial Recognition," Department of Motor Vehicles (Vermont) FAQ, http://dmv.vermont.gov/enforcement-and-safety/facial-recognition.

249. Ibid.

250. Vermont Stats. Ann. §23-1607.

251. Harper, "REAL ID: A State-by-State Update."

252. Luz Lazo, "Virginia among States Scrambling to Comply with Federal Real ID Law," *Washington Post*, May 29, 2017,

https://www.washingtonpost.com/local/trafficandcommuting/virginia-among-states-scrambling-to-comply-with-federal-real-id-law/2017/05/29/2195dbe8-3cd2-11e7-8854-21f359183e8c_story.html?utm_term=.3056522a2404.

253. Marc Holmberg, "Why Do Virginia Driver's Licenses Look Like Mugshots?" CBS 6 (Richmond), October 23, 2013, http://wtvr.com/2013/10/23/holmberg-why-do-our-virginia-drivers-licenses-look-like-mugshots/.

254. Nick Miroff, "Virginia DMV Bans Smiles in Driver's License Photos," *Washington Post*, May 28, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/27/AR2009052703627.html.

255. Rebecca Glenberg,"When It Comes to Automatic License Plate Readers, Cuccinelli Gets It Right," American Civil Liberties Union of Virginia, March 13, 2013, http://acluva.org/11129/when-it-comes-to-automatic-license-plate-readers-cuccinelli-gets-it-right/.

256. Robby Soave, "Virginia Cops Constantly Photograph Random People's License Pates," *Daily Caller*, April 14, 2014, http://dailycaller.com/2014/04/14/virginia-cops-constantly-photograph-random-peoples-license-plates/; and Tom Jackman, "Despite Cuccinelli's Advice, N. Va. Police Still Maintaining Databases of License Pates," *Washington Post*, January 16, 2014, http://www.washingtonpost.com/local/despite-cuccinellis-advice-nva-police-still-maintaining-databases-of-license-plates/2014/01/16/055ec09a-7e38-11e3-9556-4a4bf7bcbd84_story.html.

257. Office of the Governor (VA), "Veto Message on SB965," https://lis.virginia.gov/cgi-bin/legp604.exe?151+amd+SB965AG.

258. Nowrasteh and Harper, "Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate," pg. 3.

259. Rachel La Corte, "Washington Becomes Latest State to Seek Federal ID Compliance," *Seattle Times*, May 16, 2017, https://www.seattletimes.com/seattle-news/politics/washington-becomes-latest-state-to-seek-federal-id-compliance/.

260. Wash. Rev. Code. §46-20-37.

261. Matt Fikse, "Never Mind the Drones: The SPD Already Knows Where You've Been," *Crosscut*, January 24, 2013, http://crosscut.com/2013/01/24/law-justice/112617/never-mind-drones-spd-already-knows-where-youve-be.

262. Harper, "REAL ID: A State-by-State Update."

263. Linda Rosencrace, "West Virginia Uses Facial-Recognition Technology to Fight Driver License Fraud," *Computer*, January 11, 2002, http://www.computerworld.com/s/article/67328/West_Virginia_uses_facial_recognition_technology_to_fight_driver_license_fraud.

264. "Biometric Center of Excellence," Federal Bureau of Investigation, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence.

265. "Wisconsin Driver's License and ID Card Information," U.S. Citizenship and Immigration Services, https://www.uscis.gov/sites/default/files/USCIS/Verification/E-Verify/E-Verify_Native_Documents/Wisconsin_RIDE_Fact_Sheet.pdf.

266. Wisconsin State Journal KRT, "Facial Recognition System Makes Fake Licenses Hard to Get in Wisconsin," *Security InfoWatch*, May 8, 2006, http://www.securityinfowatch.com/news/10554487/facial-recognition-system-makes-fake-licenses-hard-to-get-in-wisconsin.

267. Tuccille, "30,000 Cops Can Access Ohio's Facial Recognition Database without Oversight."

268. State Sen. Mary Lazich, "Please Look at the DMV Camera and Smile," *A Legislative Column by State Senator Mary Lazich* (blog), June 16, 2009, http://archive.franklinnow.com/blogs/communityblogs/48151772.html.

269. Thomas Ahearn, "Three More States Join E-Verify RIDE Program Beginning July 31," Employment Screening Resources, August 21, 2017, http://www.esrcheck.com/wordpress/2017/08/-1/three-more-states-join-e-verify-ride-program-beginning-july-31/.

270. Tuccille, "30,000 Cops Can Access Ohio's Facial Recognition Database without Oversight."

271. "Automatic License Plate Reader FOIA Documents: Wyoming," American Civil Liberties Union, https://www.aclu.org/technology-and-liberty/automatic-license-plate-reader-foia-documents-wyoming.

272. Chief Chris Walsh, "ALPR," Casper (Wyoming) Police Department, August 6, 2012, https://www.aclu.org/files/FilesPDFs/ALPR/wyoming/alprpra_casperpd_casperwy.pdf.

RELATED PUBLICATIONS FROM THE CATO INSTITUTE

Surveillance Takes Wing: Privacy in the Age of Police Drones by Matthew Feeney, Cato Institute Policy Analysis no. 807 (December 13, 2016)

Watching the Watchmen: Best Practices for Police Body Cameras by Matthew Feeney, Cato Institute Policy Analysis no. 782 (October 27, 2015)

Checking E-Verify: The Costs and Consequences of a National Worker Screening Mandate by Alex Nowrasteh and Jim Harper, Cato Institute Policy Analysis no. 775 (July 7, 2015)

REAL ID: A State-by-State Update by Jim Harper, Cato Institute Policy Analysis no. 749 (May 12, 2014)

Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration by Jim Harper, Cato Institute Policy Analysis no. 612 (March 6, 2008)

Effective Counterterrorism and the Limited Role of Predictive Data Mining by Jeff Jonas and Jim Harper, Cato Institute Policy Analysis no. 584 (December 11, 2006)

Understanding Privacy—and the Real Threats to It by Jim Harper, Cato Institute Policy Analysis no. 520 (August 4, 2004)

CATO INSTITUTE

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. All policy studies can be viewed online at www.cato.org. Additional printed copies of Cato Institute Policy Analysis are $6.00 each ($3.00 each for five or more). To order, please email catostore@cato.org.