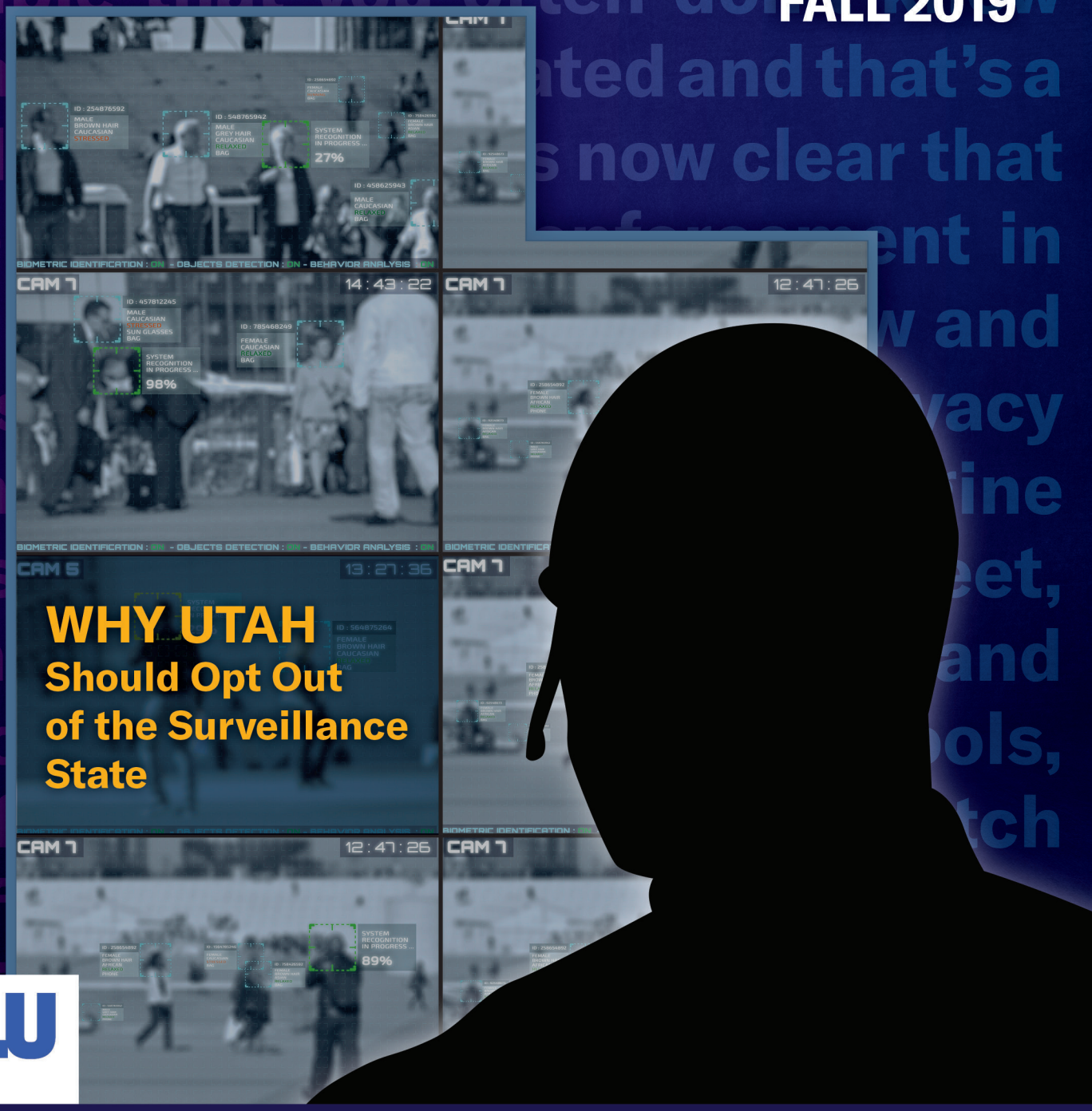
LIBERTY REPORTER

FALL 2019



ACLU Utah

Operation Rio Grande | 2020 Legislative Preview | Social Media Blocking Toolkit

State of Surveillance

To protect our right to privacy, we first need to realize what we might lose.

Imagine two streets in a Utah city.

On the first street, the neighbors know each other and talk often. They share tools, care for each other's pets, and watch out for children playing in the street. No security cameras scan the sidewalks, and people speak freely without fear of being recorded. In the evening, families go for walks to visit on front porches and talk about ways to improve their neighborhood.

But on the second street, people don't know their neighbors and never visit each other. Every house is ringed by a network of security cameras linked to a government database, and "No Trespassing" signs are planted in every yard. A police surveillance camera on a telephone pole scans passers-by with facial recognition software, while watchful eyes behind curtained windows report every strange car and person to the authorities.

Which of these streets is safer?

Which of these streets is more connected?

Which street would you prefer to live on?

"More surveillance makes us more secure."

This imagined view of two streets isn't far-fetched. The reality of the second street—where overlapping camera systems crowd out human interaction and erode privacy—could become a reality in more Utah cities if law enforcement is given permission to acquire new and more invasive surveillance systems. And in case you think cameras that can recognize your face, scanners that can see inside your clothes, and artificial intelligence software that can mine your social media posts for certain phrases are still science fiction, you should know that these systems are already here (see sidebar, *Under Scrutiny*).

One argument frequently made in favor of adding security cameras and giving law enforcement greater leeway to spy on people is that "more surveillance makes us more secure." But is that true?

The former East Germany—where one in six residents was an informer for the Stasi secret police—was one of the most surveilled nations in history. The Stasi placed hidden cameras, bugged phones, and intercepted mail to spy on its citizens. But did the East Germans feel more secure in their homes and neighborhoods, and especially in their freedom of thought and expression? One answer loudly claiming 'no' is the 5,000 people who risked their lives to escape East Germany over the Berlin Wall. In fact, the Stasi's police state more closely resembles the oppressed atmosphere of the second street in the example above. As Chad Marlow, a senior advocacy and policy counsel at the ACLU, puts it, "The real threat to public safety today is increased surveillance."

Invisible right

Of all of your civil liberties, your right to privacy is the most elusive. You can't hold it like a newspaper, invoke it like your right to a lawyer, or mark it like an election ballot. Privacy is so intangible that you often don't know when it has been violated. And that's a problem, because it is now clear that state and local law enforcement agencies in Utah have been working on new and intrusive ways to violate our privacy over the last several years. This includes the recent revelation that Utah's Department of Public Safety scanned every Utah driver's license photo thousands of times between 2015 and 2017 with facial recognition software at the request of the FBI, ICE, and out-of-state police agencies. The nature of privacy violations is that the public often doesn't learn about them—like the NSA's warrantless wiretapping revealed by Edward Snowden—until long after they started. Which also means there are likely more invasions of our collective privacy of which we are still unaware.

Fortunately, Utahns can work to reclaim their privacy from encroachment by mass surveillance. Organizations like the ACLU of Utah and the libertarian-leaning Libertas Institute are pushing back against law enforcement's demand for new and invasive technology. Joining this effort is a bipartisan team of lawmakers concerned that rapid advances in surveillance and analysis are leapfrogging the existing state codes, requiring the creation of new and better laws to regulate them. But

Under Scrutiny

Several high-profile controversies have raised warnings about increasing surveillance in Utah.

3D Body Scanners

March-May 2019

Utah's Attorney General Sean Reyes signed an agreement with Liberty Defense Technologies to allow testing of Hexwave millimeter wave body scanners at sporting events, schools, places of worship, and festivals in Utah. Press releases touted Hexwave's artificial intelligence abilities to detect weapons and explosives obscured by clothing, while AG Reyes claimed it will "push the perimeter out further" to help reveal threats. When the agreement became public in May, gun rights advocates, libertarian groups, and ACLU of Utah raised privacy concerns.

Facial Recognition Searches

July 2019

State officials went on the defensive and lawmakers expressed concerns after the *Washington Post* reported that Utah's Department of Public Safety (DPS) allowed thousands of scans of Utah driver's license and other photos with facial recognition software at the request of local and outside law enforcement. Legislative hearings in September determined the scans, overseen by Utah's Statewide Information and Analysis Center (SIAC), were conducted using outdated software, operated without legislative authority, and included images of children. New limits on facial recognition scans are expected to be introduced during Utah's 2020 legislative session.

Data Mining

August 2019

Technology start-up company Banjo faced skepticism from Utah lawmakers when it requested $2.2 million in ongoing funding to expand its Live Time Intelligence platform—an AI platform that "ingests, synthesizes, and analyzes thousands of unique data signals simultaneously" from public and government data sources, including traffic and security cameras, alarms, social media posts, and weather data. State law enforcement agencies backed the proposal, but a bipartisan group of lawmakers and civil liberties groups worried about potential abuse.

before we can enact new policies to protect our privacy, more Utahns need to understand what we lose when our right to be left alone is threatened.

No crime, no problem.

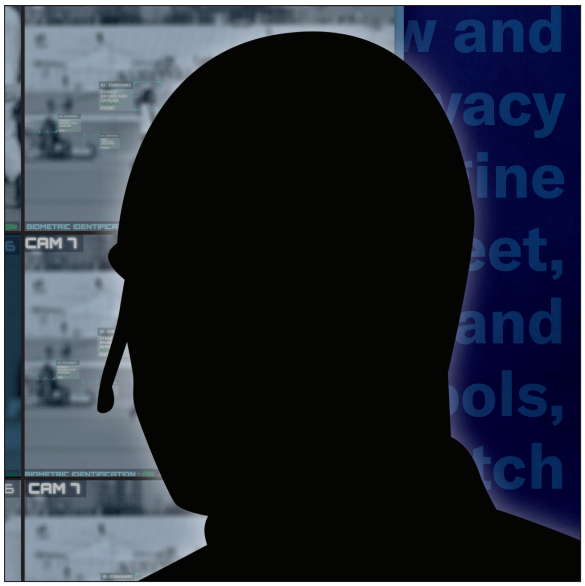
Why should you care that your local police want to spy on you? After all, if you're not breaking the law, why worry about surveillance cameras with facial recognition software or 3D body-scanners hidden in benches outside a sports stadium?

No crime, no problem. Right?

It's a fair question, and to answer it we need to examine the troubling philosophy behind the government's seeming desire to watch everyone all the time. The problem with mass surveillance is that it presumes everyone is a criminal or is about to commit a crime. Cameras with facial recognition software don't just scan and track people breaking the law. They target everyone with a face: adults, kids, and grandparents. An analogy to mass surveillance is like having a police car follow your vehicle at all times. Most of the time you're not breaking the law when you drive. But what happens when you roll through a red light a few seconds too late? Suddenly, the lights and sirens switch on behind you and you've got a ticket. Imagine a police car constantly shadowing you during a typical day, and you'll realize what it's like to live in a state of constant surveillance.

Mass surveillance also broadens the ability for police to track people's movements and activities over distance and time. Instead of a police officer sitting in an unmarked car staking out a suspicious residence, a single, well-placed camera can accomplish the same task for a dozen houses—suspicious or not—around the clock without ever needing a cup of coffee or a bathroom break. Apply facial recognition software to the camera images, and the police can determine who is coming and going from any house at any time.

Finally, new surveillance technology promises to accelerate the pace of solving crimes by replacing human work with machine learning. For example, a traditional criminal investigation to identify a suspect might require days of police work to scan fingerprints, review license plates, interview witnesses, and stake out a house. But with facial recognition software able to match camera images to a database holding millions of driver's



license photos, a computer algorithm can spit out a name and last known addresses in a few seconds. This increased efficiency is one reason why police are always requesting more surveillance. These devices save law enforcement time and effort by making it faster and easier to identify suspects. And their argument would make sense if the high-tech tools they used worked as reliably as advertised.

False positives

To justify their acquisition of new surveillance technology, law enforcement agencies often claim these tools are more accurate and less intrusive than prior methods. But independent test results reveal these products regularly overpromise and underdeliver. The oldest and most commonplace of these systems, airport body-scanners, routinely fail to function accurately for people who aren't white and male or people with unique clothing or hair styles. And even the most advanced facial recognition algorithms are rife with systematic errors against minority populations. A 2018 test by the ACLU demonstrated how Amazon's Rekognition software, a popular facial recognition program used by law enforcement, wrongly matched photos of 28 Members of Congress to mugshots of people who had been previously arrested, falsely tagging people of color at higher rates. Plus, earlier this year, body-camera maker Axon rejected adding

Continued on page 11

Key Definitions

Artificial Intelligence (AI): Computer software that analyzes camera images to identify people, vehicles, objects, and weapons. Higher-level AI software can be programmed to "learn" from past experiences to reduce errors, increase accuracy, and predict future behavior.

Biometrics: Identifiable characteristics based on physical attributes like fingerprints, facial features, voice, DNA, and body dimensions.

Facial Recognition: Software that measures facial textures and dimensions, such as the gap between the eyes and the distance from forehead to chin, to match camera images to a database of known facial profiles—confirming a person's "faceprint."

Fourth Amendment: An amendment to the U.S. Constitution ratified in 1791 as part of the Bill of Rights that prohibits unreasonable searches and seizures of property by the government, including law enforcement. It forbids arrests without probable cause, and regulates the use of search warrants, wiretaps, and other forms of surveillance.

Rap Back: An FBI service that continually reviews a person's criminal history without requiring repeated background checks. Originally designed to monitor records for teachers, daycare workers, and other people in positions of trust, Rap Back is now used by state and local authorities within Utah to constantly scan for criminal record updates for people in government databases.

Statewide Information and Analysis Center (SIAC): The division of Utah's Department of Public Safety (DPS) that collects and analyzes images from multiple databases, including driver's licenses, state IDs, and booking photos, using facial recognition software.

ABORTION, continued from page 4

causing some of our supporters to forget that Utah is embroiled in a legal battle to keep abortion safe and accessible. Our attorneys have been very busy, however. On June 20, the court granted the state defendants' request for discovery, a legal process where both sides seek documents and other information related to the case. Both the ACLU of Utah and Planned Parenthood opposed the state's request for discovery because it would unnecessarily delay the resolution of the lawsuit. Although the court granted the state's

request for partial discovery, the judge stressed that the decision did not reflect how he would ultimately rule in the case. Since that time, our attorneys have been engaged in gathering documents and other discovery actions, which has lengthened the lawsuit by several months. However, by February 2020, we expect to be able to ask the court for summary judgment—making our case for a final ruling that Utah's 18-week abortion ban is unconstitutional.

SURVEILLANCE, continued from page 7

facial recognition features to their devices, citing "evidence of unequal and unreliable performance across races, ethnicities, genders and other identity groups." Closer to home, Liberty Defense Technologies, the Massachusetts company that partnered with Attorney General Sean Reyes to test Hexwave 3D body scanners in Utah, warned potential partners "to use caution and not rely in any way on the correct functioning, effectiveness or performance of Hexwave." Their warning is even more alarming when combined with the fact that these scanners are designed to be hidden in public places, allowing, as Reyes stated, "to potentially push the perimeter out further." This wide-open approach to surveillance in and near public places should not only alarm the 260,000 Utahns with concealed firearm permits, but also anyone with a wearable or implanted medical device, because most scanners can't distinguish between a gun and a colostomy bag. For instance, a man who a body scanner identifies as acting erratically with a suspicious bulge at his waist might be a diabetic with a malfunctioning insulin pump. If security guards trust that the artificial intelligence running the scanner is accurate, they could target this person as an armed threat when he is actually suffering from a medical emergency.

Lastly, law enforcement backers of increased surveillance often assert these tools will speed the resolution of kidnappings, terrorist attacks, and other high-profile but rare crimes. And while these claims may be true, policymakers need to balance these exceptional situations with the widespread privacy violations that cameras on every street corner inflict on the whole population all the time. For obvious reasons, it's not wise to create policies dependent solely on extreme scenarios, otherwise our building codes would be based on asteroid impacts.

Our role

Utah is currently experiencing a surveillance revolution led by intrusive body scanners, more security cameras, facial recognition software, and artificial intelligence algorithms that link them all together. Recent headlines demonstrate that these systems are already at work in our communities, whether we know it or not. But Utah can also join a different revolution that is pushing back against a surveillance state. We can demand new regulations and limits on how deeply the government can peer into our private lives. We can start a new and broad discussion about the need to balance security, due process, and privacy rights. And when state and local police departments propose new and truly invasive surveillance systems, we can make sure the process is transparent, that our privacy is protected, and that the shiny new technology actually works. Otherwise, we will end up living under the dome of surveillance on the second street mentioned at the start of this article, thinking we are safe, but actually feeling very insecure.

PREVIEW, continued from page 9

***Q:** What bill are you most excited about working on next year?*
ML: Criminal justice bills are always exciting because of the opportunities to collaborate with diverse partners, as well as the potential to change people's lives for the better. I am also keen to work on several bills focused on gender equality. These bills will ensure that women who are incarcerated have access to vital medications, create paid family leave policies, and promote a Constitutional amendment that elevates the rights of women in our state to an equal footing.

***Q:** Why does the ACLU lobby the legislature?*
ML: From an efficiency standpoint, it makes more sense to improve a bill as it moves through the legislative process rather than wait until it becomes law and challenge it in court. Plus, the courts are not the best place to promote positive legislation—like the limits on facial recognition we will seek next session.

***Q:** How is the second session of a two-year term different from the first one?*
ML: On one hand, lawmakers are more likely to propose legislation during this second session because they know the system better and have closer relationships with their colleagues. But on the flip side, 2020 is an election year—with all the perils that brings.

***Q:** What advice would you give to someone who wants to follow the 2020 session?*
ML: The Utah legislature is known for being accessible and easy to follow, starting with the award-winning website (www.le.utah.gov) that makes it easy to track legislation and hearings. But our part-time legislators are also approachable, and most are very happy to hear from their constituents. Right now, before the session begins in January, is an excellent time to contact your representatives and tell them what's on your mind.