GEORGETOWN LAW
Center on Privacy & Technology

Statement of Harrison Rudolph, Associate

Center on Privacy & Technology at Georgetown Law

Before the

Utah State Legislature

Government Operations Interim Committee

Meeting on

Facial Recognition Technology Use

Wednesday, September 18, 2019

For more information, contact Harrison Rudolph at hsr11@georgetown.edu or (202) 661-6709.

Executive Summary

Nearly every Utah adult has been affected by police face recognition. According to records disclosed by the Department of Public Safety (DPS), the Statewide Information & Analysis Center (SIAC) has routinely searched *over 5 million* Utah driver's license and state identification card photos without a warrant.

The best way to protect the public from face recognition is for Utah to hit the pause button.

In 2015, the Center on Privacy & Technology at Georgetown Law investigated the privacy, civil liberties, and civil rights protections in face recognition systems used by the FBI and police nationwide. We published our findings in *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, available at www.perpetuallineup.org/report. In 2017, we investigated the privacy, civil liberties, and civil rights implications of the Department of Homeland Security's use of face recognition technology at international airports. We published our findings in our report, *Not Ready for Takeoff: Face Scans at Airport Departure Gates*, available at www.airportfacescans.com. In 2019, we investigated real-time face surveillance in *America Under Watch: Face Surveillance in the United States*, available at www.americaunderwatch.com, and we investigated misuse of face recognition by police in *Garbage In, Garbage Out: Face Recognition on Flawed Data*, available at www.flawedfacedata.com.

A few key takeaways from my testimony are below:

Problems

- **Unprecedented police power.** Face recognition gives police a power that they never had before. Face recognition is unique from familiar police technologies in at least three critical ways:
    - Face recognition gives police the ability to surveil, in secret, virtually every Utah adult who steps out in public;
    - By routinely scanning Utah drivers' faces, DPS has access to a perpetual line-up of *law-abiding*—not just criminal—Utahns; and
    - DPS has made it virtually impossible for an ordinary Utahn to opt-out or avoid face recognition searches because DPS uses driver's licenses, which most Utahns need for driving to work, school, health care, and more.

- **Civil rights threat.** Police face recognition threatens Utahn's privacy, civil rights, and civil liberties. Surveillance chills free speech; it especially chills dissenting or unpopular voices. Prosecutors' failure to disclose police use of face recognition to criminal defendants threatens due process of law.

- **Error-prone, race- and gender-biased.** With face recognition technology, the point isn't whether you *are* a criminal, but whether an error-prone and potentially biased algorithm thinks you *look* like a criminal. Research has repeatedly shown that error-prone face recognition makes more mistakes—more misidentifications—when it's used on people of color and women.

- **Subversion of Utah's will.** The federal government is subverting state will by requesting searches of Utahn's faces without the legislature's express permission. It does not appear that the Utah Legislature has ever given DPS express permission to be conducting these searches, either.

- **Legal Vacuum**. Despite police face recognition's serious risks, including surveillance, misidentification, and bias, existing law places few restrictions on its use. Utah DPS routinely conducts warrantless searches of Utah driver's license photos using face recognition technology.

Solution

- **Hit pause.** Utah should hit the pause button on face recognition by enacting a moratorium on its use by law enforcement. Utah is a lodestar for acting to protect residents from new technologies when federal laws and federal courts have not kept pace. Despite the serious risks and harms, federal law and the federal courts have been silent on face recognition.

I. Police face recognition in Utah.

Face recognition is the automated process of comparing images of faces to determine whether they represent the same individual.[1] **Using a driver's license photo database, face recognition can reveal a person's identity**. Utah DPS contracted with Hummingbird Communications in 2008 for face recognition software.[2] Hummingbird offered to "Identify both known and unknown individuals in less than 10 Seconds" using sources including "Surveillance Images, Video, Drivers License, Booking Photos, Scanned Images, Police Artist Sketches, Internet Video (U-Tube), social network sites, Face Book, blogs or any image from any number or variety of sources."[3]

SIAC has routinely searched the Utah Driver's License Database. Between 2015 and 2017, records show that SIAC conducted more than 1,000 warrantless face recognition searches of Utah drivers on behalf of federal agencies, including the Federal Bureau of Investigation and U.S. Immigration and Customs Enforcement.[4] This is in addition to hundreds of face recognition searches conducted on behalf of state and local law enforcement agencies nationwide, too.

SIAC does not appear to have required any suspicion of wrongdoing for face recognition searches. SIAC does not appear to have required individualized, reasonable suspicion of a crime to conduct a face recognition search. According to SIAC's 2011 Policy and Procedures, SIAC only required that face recognition searches be limited to being part of an active, criminal law

[1] For a more complete discussion of this, *see* Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, T*he Perpetual Line-Up: Unregulated Police Face Recognition in America*, 28 (2016), https://www.perpetuallineup.org/report (hereinafter "The Perpetual Line-Up").

[2] *See* State of Utah Contract, #096227, DPS Department of Technology Services, 12/22/2008.

[3] *See* Hummingbird Communications, *Response to Solicitation JG9031*, 11/23/2008.

[4] *See* Drew Harwell, *FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches*, The Washington Post, 7/7/2019.

enforcement investigation.[5] This is below a "warrant" standard, below the "probable cause" standard, and below the "reasonable suspicion" standard.

SIAC may have searched against children's faces using face recognition technology. SIAC has used face recognition to search against state identification card photographs,[6] which DLD issues to residents of any age.[7] While DLD has asked parents to sign for children under sixteen (16) years of age obtaining a state identification card, we have not seen evidence that the DLD notified these parents that they are enrolling their children into a face recognition database.

II. Face recognition gives police unprecedented power.

Face recognition enables law enforcement agencies to obtain virtually every Utah adult's identity without their knowledge or consent. Face recognition technology allows police to identify groups of Utahns remotely and in secret. The FBI and Utah police would violate Utah law and the U.S. Constitution by secretly pickpocketing protesters at a Second Amendment rally and identifying them from their driver's license photos. Nor can the FBI or Utah police secretly fingerprint a crowd of gun control protesters from across the street. Face recognition—in essence—could allow the FBI and police to do each of these things. That is unprecedented.

Face recognition technology allows police to identify virtually any Utah adult who steps out in public—not just criminals. According to documents disclosed by SIAC, its face recognition database is composed of more than 5 million driver's photographs. This represents a sweeping expansion of law enforcement access to personal data. Never before have state and local police departments, or the FBI, had the ability to run biometric searches against a majority of their state's citizens when conducting routine investigations. In fact, Americans have repeatedly rejected efforts to create national identification databases. President Ronald Reagan is reported to have likened proposals to create a national ID system in 1981 to the biblical "mark of the beast."[8] President Bill Clinton dismissed a similar measure because the idea invoked "Big Brother."[9]

Face recognition technology is virtually impossible to avoid. It is virtually impossible for Utahns to avoid face recognition because DPS has adopted face recognition technology on driver's license and state identification card photos, and for most Utahns, driving is necessary to keep a job or take a child to school. Opting out of face recognition is—simply put—not an option. Nor can Utahns wear a Halloween mask each time they step outdoors. The only choice is to be subject to face recognition technology.

III. Face recognition threatens Utahn's rights.

---

[5] *See* Utah SIAC, *Policy and Procedures: Facial Recognition System*, 10-31-2011.

[6] *See* SIAC, *Facial Recognition System Flyer* ("Currently there are over 5 million Utah driver license & state identification card photos as well as 500,000 booking images from various Utah jails and prisons enrolled in the system.").

[7] *See* Utah Department of Public Safety, *Identification Card*, https://dld.utah.gov/licensingid-cards/identification-card/ ("Anyone of any age can obtain an identification card. Although, persons under 16 years of age must have a parent or legal guardian sign for them. DPC applicants are not eligible for an identification card.").

[8] *See* Stephen Moore, *The National ID Card: It's Baaack!,* Cato Institute (Sept. 23, 1997), https://www.cato.org/publications/commentary/national-id-card-its-baaack.

[9] *See* ACLU, *Broad Coalition Urges President Obama and Congress to Oppose Biometric National ID* (Apr. 13, 2010), https://www.aclu.org/press-releases/broad-coalition-urges-president-obama-and-congress-oppose-biometric-national-id.

Face recognition technology threatens Utahn's privacy and First Amendment rights. Law enforcement agencies acknowledge the serious chilling effect of face recognition surveillance on free speech and assembly. The International Justice and Public and Safety Network (Nlets) observed in 2011 that "[t]he public could consider the use of facial recognition in the field as a form of surveillance … The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition."[10] Face recognition technology, Nlets wrote, should never be used in the field as a "ubiquitous system that is covertly deployed and used to identify people without their consent or knowledge."[11]

Face recognition technology threatens Utahn's right to due process of law. Face recognition can produce evidence material to a defendant's guilt or innocence. While SIAC, for its part, acknowledges that face recognition searches can ultimately lead to a suspect's "arrest, conviction…"[12], prosecutors rarely disclose face recognition use to the criminally accused. In 1963, the United States Supreme Court held in *Brady v. Maryland* that suppression of evidence material to the guilt or innocence of the accused violates his due process rights under the Fourteenth Amendment.[13] As conducted by law enforcement, face recognition searches produce *Brady* evidence and failures to disclose threaten due process of law.

Face recognition searches can also produce exculpatory *Brady* evidence. SIAC's face recognition searches actually return whole galleries of *multiple* drivers' faces. For example, SIAC returns between ten (10) and twenty (20) drivers' faces in response to FBI requests for searches[14]—the accused rarely find that out, either. Consider what one analyst responsible for Washington Country, Oregon's face recognition system described: "We found in our testing that something that returned a 99% wasn't the person …. And some results that returned 73% were indeed that person."[15] In both of these examples, the face recognition algorithm concluded that at least one person looked *more* like the suspect than the person arrested and charged.[16] Yet the full candidate list—even if it contained 19 or more people considered by the algorithm *more likely* to be the suspect—is likely never seen by the defendant.

---

[10] Nlets, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field*, 17 (June 30, 2011), *available at* https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf (Internal cites omitted. The privacy impact assessment was drafted by the Nlets Facial Recognition Workgroup, composed of practitioners from the FBI, New Jersey State Police, Illinois State Police, North Carolina DMV, Pinellas County Sheriff's Office, Delaware State Police, Automated Regional Justice Information System, Oregon State Police, New York State DMV, County of Cumberland District Attorney's Office, and the Chicago High Intensity Drug Trafficking Area.)

[11] *Id.*

[12] *See* Utah SIAC, *Policy and Procedures: Facial Recognition System*, 10-31-2011.

[13] *See* Brady v. Maryland, 373 U.S. 83, 87 (1963).

[14] *See* Utah's DPS/FACE Services Unit, *Memorandum of Understanding, Procedures*.

[15] *See* On Point, *San Francisco Bans Facial Recognition Tech Over Surveillance Bias Concerns*, On Point (May 16, 2019), https://www.npr.org/podcasts/510053/on-point.

[16] It also means that the rank order of the candidate list may not reliably indicate who is more or less likely to be a match. As a consequence, the entire list should be turned over to the defense in all cases, regardless of the defendant's place in that rank order.

IV. Face recognition can misidentify innocent people and its mistakes disproportionately affect women and people of color.

Face recognition technology can falsely identify innocent Utahns as suspects. When face recognition *fails* to identify a suspect, it may actually *misidentify* an innocent person. For example, Sri Lankan authorities relying on face recognition technology mistook an innocent American college student for a woman suspected of participating in the 2019 Sri Lanka Easter bombings.[17] Partly, that is because the accuracy of a face recognition system is highly dependent on the quality of the "probe" photograph it uses to conduct its search. Poor quality photos—grainy surveillance footage, poor lighting, faces that are obscured or turned away from the camera—will generally produce less reliable results than high quality face photographs.[18]

Face recognition technology performs worse on women and people of color. Research over the last decade has consistently shown that that face recognition technology performs worse on women and people of color. Last year, the American Civil Liberties Union (ACLU) tested Amazon's face recognition product, "Rekognition," and found that Rekognition's face identification tool falsely matched the faces of people of color with photos in a mugshot database at a disproportionately high rate.[19] Massachusetts Institute of Technology (MIT) researchers Joy Buolamwini and Timnit Gebru conducted a study finding that three commercially available gender classification algorithms all produced the highest error rates (20.8%–34.7%) when analyzing the faces of women with darker skin.[20] These findings align with earlier research. In 2012, a team of scientists—including an FBI technologist—studied three commercially available face recognition algorithms and found that all three algorithms performed significantly worse on faces of women than on faces of men, on faces of African Americans than on faces of other races, and on faces in the age range 18 to 30 than on older faces.[21]

V. The federal government is subverting Utah's will by requesting searches of Utahn's faces without the legislature's express permission.

Utah's legislature has never authorized federal requests for, or DPS execution of, face recognition searches. When DPS reached a Memorandum of Understanding (MOU) with the FBI on face recognition search requests, DPS relied on the Government Records Access and Management Act for its authority.[22] That law was enacted all the way back in 1991—before police face recognition existed and before the Utah legislature could have contemplated its use.[23]

---

[17] *See* Jeremy C. Fox, *Brown University Student Mistakenly Identified as Sri Lanka Bombing Suspect*, Boston Globe, Apr, 28, 2019, https://www.bostonglobe.com/metro/2019/04/28/brown-student-mistaken-identified-sri-lanka-bombings-suspect/0hP2YwyYi4qrCEdxKZCpZM/story.html.

[18] For a more complete discussion of this, *see* The Perpetual Line-Up.

[19] Jacob Snow, ACLU, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[20] Joy Buolamwini & Timnit Gebru, *Gender Shades*, 81 Proceedings of Machine Learning Research 1, 11 (2018).

[21] Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge, & Anil K. Jain, *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics & Sec. 1789 (2012).

[22] *See* Utah's DPS/FACE Services Unit, *Memorandum of Understanding, Procedures*.

[23] MuckRock, *Government Records Access and Management Act (GRAMA)*, Utah Public Records Guide, https://www.muckrock.com/place/united-states-of-america/utah/.

That is not legislative intent. The Utah Legislature has never given the FBI or ICE its express permission to be requesting searches of Utah drivers' faces. It does not appear that the Utah Legislature has ever given DPS express permission to be conducting these searches, either.

VI. Police face recognition operates under few, if any, legal limitations.

Police use of face recognition technology operates in a legal vacuum. Neither the Utah Legislature nor the U.S. Congress have enacted comprehensive regulation of police use of face recognition technology. That means the technology's risks for surveillance, misidentification, and bias remain unchecked. Recently, the cities of San Francisco, California and Somerville, Massachusetts have enacted bans on police face recognition use.[24] Portland, Oregon may be considering a wholesale ban on the technology across the public and private sectors.[25] Oregon and New Hampshire prohibit face recognition on police body cameras;[26] Maine and Vermont restrict police face recognition use in conjunction with drone footage;[27] several states restrict police access to search driver's license face recognition systems.[28]

Federal courts have not considered whether police face recognition violates the Fourth Amendment. **A Supreme Court decision is unlikely to come soon**. No federal court has adjudicated the question of whether a warrantless face recognition search violates the Fourth Amendment of the U.S. Constitution. (In part, that may be because prosecutors rarely disclose use of face recognition to criminal defendants.) That means a holding from the Court on the question is unlikely to arrive quickly. For example, according to the Electronic Frontier Foundation, it took approximately eight (8) years from the first federal court's decision in 2010 for the U.S. Supreme Court, in 2018, to hold in *Carpenter* that a warrant was typically required to obtain a suspect's historical cell site location data.[29]

VII. Utah leads the nation in protecting its residents from invasive new technologies when federal laws and federal courts cannot keep pace. Utah should hit the pause button on police face recognition.

Utah is a lodestar for protecting residents in the face of invasive new technologies and federal inaction. For example, the Utah Legislature has passed laws to protect Utah residents from law enforcement access to third-party data, cell site simulators, radar imaging devices, and GPS tracking. On face recognition, Utah has a chance to lead the way again.

---

[24] Caroline Haskins, *A Second U.S. City Has Banned Facial Recognition*, Vice, 6/27/2019, https://www.vice.com/en_us/article/paj4ek/somerville-becomes-the-second-us-city-to-ban-facial-recognition.

[25] Kate Kaye, Portland officials want to ban private use of facial recognition technology, citing 'accuracy problems', GeekWire, 9/5/2019, https://www.geekwire.com/2019/portland-officials-want-ban-private-use-facial-recognition-technology-due-accuracy-problems/.

[26] Or. Rev. Stat. § 133.741(1)(b)(D); N.H. Rev. Stat. Ann. § 105-D:2(XII).

[27] Vt. Stat. Ann. tit. 20 § 4622(d)(2); Me. Rev. Stat. Ann. tit. 25 § 4501(5)(D).

[28] Me. Rev. Stat. Ann. tit. 29-A, § 1401; Mo. Ann. Stat. § 302.189; N.H. Rev. Stat. Ann. § 260:10-b and N.H. Rev. Stat. Ann. § 263:40-b; Vt. Stat. Ann. tit. 23, § 634(c).

[29] *See* Electronic Frontier Foundation, *CSLI Cases*, 3/29/2019, https://www.eff.org/criminaldefender/cell-site-location/cases; *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

Utah should enact a moratorium on the use of face recognition technology by police. Face recognition is already more pervasive and more advanced than most Americans realize. Yet it continues to have, according to the general counsel of the National Security Agency (NSA) in last week's *New York Times*, "persistent imperfections" and we are "far from figuring out its proper role in our society."[30] "[T]he windows," Glenn S. Gerstell wrote, "for how long it takes for technology to shape society … are becoming almost impossibly compressed." Gerstell, for his part, criticized the "confused spate of lawsuits and statutes seeking to regulate [face recognition's] use." But in Utah, there is an opportunity to lead the way without any confusion: A moratorium on police face recognition to stave off the very serious risk that it "shape[s] society" in an "impossibly" fast way that is harmful, race- and gender-biased, and anti-democratic.

[30] Glenn S. Gerstell, *I Work for N.S.A. We Cannot Afford to Lose the Digital Revolution*, The New York Times, 9/10/2011, https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html.