

Memo to the Chief of Police:
Best Practices for Utilization of Surveillance and Biometric Technologies

Benjamin T. Moszkowicz

School of Professional and Continuing Education, University of San Diego

LEPS-530: Public Safety Law

Dr. Erik Fritsvold

February 22, 2021

TO: CHIEF OF POLICE, ANYTOWN POLICE DEPARTMENT

FROM: BENJAMIN MOSZKOWICZ, CAPTAIN, SPECIAL PROJECTS AND
LEGISLATIVE AFFAIRS, ANYTOWN POLICE DEPARTMENT

SUBJECT: Best Practices for Utilization of Surveillance and Biometric Technologies

Every day, the movements of our fellow community members are being monitored and recorded by Smart Streetlights. The technology exists to analyze this and other videos to identify individuals based on their physical characteristics. Despite not having settled case law or precedent regarding the use of these technologies, we can make inferences by reviewing other jurisdictions' legislation.

While citizens may trust video surveillance and facial recognition technologies to allow them the convenience of unlocking their cell phones, use by law enforcement to identify suspects will likely strike fear into their hearts. This presents a unique opportunity for the department to educate, demonstrate transparency, and collaborate with the community to address implementation.

Functionality Overview

Surveillance and biometric technologies have tremendous power to revolutionize the way we investigate and solve crimes. Smart Streetlights stand as modern-day sentinels, constantly recording a buffer of potentially valuable data that remains reviewable days later. Facial recognition technology can analyze a photo and scan against millions of known subjects, producing a list of possible matches to lead investigators.

In addition to cost-effective LED lighting, 3,200 Smart Streetlights in San Diego, California, are equipped with video cameras that record 24 hours per day. Since implementation in 2018, videos have helped solve over 400 crimes (Holder, 2020). Officials there have found several benefits from the technology, including (City of San Diego Public Meeting, 2019, slide 9):

- Increased Conviction Rate
- Reduced investigation costs
- Increased plea bargain over trial
- Improved cost recovery
- Time saved from incident to prosecution
- Reduced police department lawsuits
- Reduced gun violence
- Cost savings from reduced crime

Facial recognition technology uses can vary from identifying suspects in investigations to controlling access to secured areas ranging from businesses to international borders. It can search large crowds very quickly to find specific people and can even help identify victims of child abuse (Klosowski, 2020). Over the past year, to help identify suspects, officers from Colorado to South Carolina have used this technology to compare suspect photos against driver's licenses (Schmelzer, 2020) and previous arrest photos (Bland, 2020).

Facial recognition technology has been in use since 2001 (Klosowski, 2020); however, no legislative guidance on these technologies exists in Anytown. As such, I

have reviewed similar regulatory structures (both proposed and currently in place) from across the nation.

Legislation Review and Inference

A recently proposed bill in the United States Senate would prevent federal law enforcement entities from using facial recognition technology.¹ While the legislation was unsuccessful, it may be a bellwether of the current Democrat-led congress. As written, the legislation would also preclude state and local agencies from receiving several federal grants unless they adopt similar policies or laws (Solon, 2020).

While no federal law yet exists, several states have undertaken legislation to explicitly protect their citizens' privacy rights. In 2008, Illinois was the first state to enact its Biometric Information Privacy Act, which "regulate[s] the unlawful collection and storage of biometric information including photos of faces" (Klosowski, 2020). Over a decade later, on October 8, 2019, Governor Gavin Newsom signed California AB-1215, which effectively restricted law enforcement from using any biometric surveillance system.²

Despite, or perhaps due to the lack of federal- or state-imposed oversight, several local jurisdictions have limited the use of facial recognition technology. Cities from San Francisco, California, to Boston, Massachusetts, have ordinances that prevent law enforcement and other government agencies from using facial recognition technologies (Klosowski, 2020). On September 10, 2020, the Portland City Council banned the use of facial recognition technology. The ban now even extends to areas

¹ The failed legislation was entitled, the Facial Recognition and Biometric Technology Moratorium Act of 2020

² California Assembly Bill 1215 defines a biometric surveillance system as, "any computer software or application that performs facial recognition or other biometric surveillance." AB1215 (2019)

open to the public in private businesses operating in the city. Portland Commissioner Jo Ann Hardesty, who introduced the bill, described it as "model legislation" for the rest of the country (Bailey Jr., 2020).

Community Engagement Strategies

In 2018, the City of San Diego installed Smart Streetlights. Despite the San Diego Police Department learning about the streetlights' capabilities after implementation, they faced severe backlash from the community and privacy rights groups (Holder, 2020). As Anytown now finds itself similarly situated, the following recommendations reflect our department's opportunity to learn from San Diego and engage the community proactively to help develop policies to guide our use of these new technologies.

- Publish a map detailing Smart Streetlight locations. Include how Anytown chose the sites.
- Do not actively monitor cameras, and make recordings available through existing public records request procedures (City of San Diego Public Meeting, 2019, slide 10).
- Require command approval for any recovery or review of recordings.
- To demonstrate proactive transparency, disclose within 30 days when downloading from lights in a particular zone or area. Publish disclosure on our public website, including the date and time range downloaded.
- Ensure our policy does not "invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists" (Holder, 2020).

- Create a reasonable retention policy for all recordings. Access to videos is limited to five days. Delete all videos not downloaded as evidence by then (Holder, 2020).

In addition to these recommendations, the department should integrate into policy the following five principles for facial recognition as proposed by the International Association of Chiefs of Police (IACP, 2019):

1. Develop usage policies following the law.
2. Policies must protect constitutional rights.
3. Realize results may include a list of candidates of a different race, gender, or age than the exemplar photo.
4. Ensure results are for investigative lead purposes only, never probable cause.
5. Before using the technology, users must undergo training to understand how it works.

Conclusion

Ultimately, to harness the power emerging technology can have to make our community safer, we must educate and engage with the community to spread awareness and promote collaboration on policy formation. As Richland County Sheriff Leon Lott suggested, "Ensure the public understands what the technology is and is not. It only provides us with a lead. You then have to verify that you have the right person. No one is ever arrested based on facial recognition technology alone" (Smith Jr., 2020).

While not everyone will agree with every decision, we must solicit and consider input before making the best choices for the community. Our department has a unique opportunity to learn from other jurisdictions' experiences, bolster public trust, and demonstrate transparency in policymaking and policing.

//signed// Captain Benjamin Moszkowicz

Special Projects and Legislative Affairs

References

- AB1215. (2019). California Assembly Bill 1215, Relating to Law Enforcement.
Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215
- Bailey Jr., Everton. (2020, Sep 10). Portland approves strictest ban on facial recognition technology in the U.S. The Oregonian / Oregon Live. Retrieved from <https://www.oregonlive.com/politics/2020/09/portland-approves-strictest-ban-on-facial-recognition-technology-in-the-us.html>
- Bland, David. (2020, Aug 3). S.C. Agencies Use Facial Recognition to Identify Rioters. Police One. Retrieved from <https://www.police1.com/george-floyd-protest/articles/sc-agencies-use-facial-recognition-to-identify-rioters-ilvvlqlcVPBgK83k/>
- City of San Diego Public Meeting. (2019, Sep 10). Smart Streetlights [Powerpoint slides]. Retrieved from <https://www.sandiego.gov/sites/default/files/sust-smartstreetlightpublicmeeting-091019.pdf>
- Holder, Sarah. (2020, Aug 6). In San Diego "Smart" Streetlights Spark Surveillance Reform. Bloomberg City Lab. Retrieved from <https://www.bloomberg.com/news/articles/2020-08-06/a-surveillance-standoff-over-smart-streetlights>
- IACP. (2019, July). Guiding Principles for Law Enforcement's Use of Facial Recognition Technology. International Association of Chiefs of Police. Law Enforcement Imaging Technology Task Force. Retrieved from <https://www.theiacp.org/sites/default/files/2019-10/LE%20Facial%20Rec%20Guiding%20Principles%20Document%20July%202019.pdf>

Klosowski, Thorin. (2020, July 15). Facial Recognition is Everywhere. Here's What We Can Do About It. New York Times. Retrieved from <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>

Schmelzer, Elise. (2020, Sept 27). How Colorado law enforcement quietly expanded its use of facial recognition. The Denver Post. Retrieved from <https://www.denverpost.com/2020/09/27/facial-recognition-colorado-police/>

Smith Jr., W. Thomas. (2020, Aug 13). Facial recognition an effective investigative tool, not big brother. Police One. Retrieved from <https://www.police1.com/police-products/police-technology/police-software/facial-recognition/articles/facial-recognition-an-effective-investigative-tool-not-big-brother-XUjt1nBNz1SbVHJ5/>

Solon, Olivia. (2020, June 25). Facial recognition bill would base use by federal law enforcement. NBC News. Retrieved from <https://www.nbcnews.com/tech/security/2-democratic-senators-propose-ban-use-facial-recognition-federal-law-n1232128>