# Minnesota Coalition on Government Information (MNCOGI)
# Reference materials for MNCOGI testimony

## Legislative Commission on Data Practices
## November 30, 2021

## Case Law References

### *Leaders of A Beautiful Struggle v. Baltimore Police Department*
### (Fourth Circuit Court of Appeals, 2021)

"On the merits, because the AIR [aerial surveillance] program enables police to deduce from the whole of individuals' movements, we hold that accessing its data is a search, and its warrantless operation violates the Fourth Amendment. Therefore, we reverse and remand."

"In *Carpenter v. United States* (2018), the Supreme Court repeated that "[t]he 'basic purpose of this Amendment' . . . 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'" (quoting *Camara v. Mun. Ct. of City & Cnty*. (1967)). "The Founding generation crafted the Fourth Amendment as a 'response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'"

"In *United States v. Jones* (2012), location-tracking technology crossed the line from merely augmenting to impermissibly enhancing. There, police used a GPS-tracking device to remotely monitor and record a vehicle's movements over 28 days. Although the case was ultimately decided on trespass principles, five Justices agreed that "longer term GPS monitoring . . . impinges on expectations of privacy." (Sotomayor, J., concurring). Based on "[t]raditional surveillance" capacity "[i]n the precomputer age," the Justices reasoned that "society's expectation" was that police would not "secretly monitor and catalogue every single movement of an individual's car for a very long period."

"The AIR program's surveillance is not "short-term" and transcends mere augmentation of ordinary police capabilities. People understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time. See *Maynard,* 615 F.3d at 560 ("It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work.”). But capturing everyone’s movements outside during the daytime for 45 days goes beyond that ordinary capacity.”

## *Carpenter v. United States*
## (United States Supreme Court 2018)

“The Government’s acquisition of Carpenter’s cell-site records was a Fourth Amendment search.”

“A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which “hold for many Americans the ‘privacies of life”—contravenes that expectation.”

“When an individual “seeks to preserve something as private,” and his expectation of privacy is “one that society is prepared to recognize as reasonable,” we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.”

“Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings “of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted.” *Carroll v. United States*, 267 U.S. 132, 149 (1925) … We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to “assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

## Other Resources

United States Government Accountability Office, August 2021: “Facial Recognition Technology, Current and Planned Use By Federal Agencies”
https://www.gao.gov/assets/gao-21-526.pdf

MIT Technology Review, August 24, 2021: “US government agencies plan to increase their use of facial recognition technology”
https://www.technologyreview.com/2021/08/24/1032967/us-government-agencies-

plan-to-increase-their-use-of-facial-recognition-technology/

Center for Security and Emerging Technology, March 2, 2021: "China's "Sharp Eyes" Program Aims To Surveil 100% of Public Space"
https://cset.georgetown.edu/article/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space/

National Public Radio, January 5, 2021: "Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State'"
https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta

## Previous MNCOGI Testimony on Facial Recognition Technology
## Legislative Coordinating Commission
## Data Practices Subcommittee
## November 7, 2019

Thank you Mister Chairman. Matt Ehling, Minnesota Coalition on Government Information. Thank you for the opportunity to provide some comments about facial recognition technology. This is an area that is largely unregulated in Minnesota at present, although the technology has been mentioned in at least one bill heard by this body - the drone bill heard previously by this subcommittee. Since comprehensive regulation of this area has yet to arrive, we would like to highlight some policy issues that the legislature may wish to address going forward.

**Facial Recognition Technology: What is it?**
First, let's define what it is we're talking about. In its simplest form, facial recognition technology is a computerized process that aims to replicate what humans can do innately - that is, review two independent photographic images, and then make a judgment call about whether or not the same individual is depicted in the two separate photographs.

A facial recognition process takes two data sets - one set containing an "unknown" image or images - and one data set of images that have known, identifying information attached. An "unknown" image, for instance, might be a video frame captured by a gas station security camera, while a "known" set of images might be a database of booking photos maintained by a local police department. Both data sets are then imported and evaluated by the facial recognition software, which analyzes multiple so-called "biometric" characteristics as it seeks to find an image match - thus linking known information to the previously unknown image.

These technological capabilities have been in development for many years, and have been piloted in several forms, at different points in time. Recent advances in the computer algorithms that underpin facial recognition software, as well as improvements in computing power and scale - have made the commercialization of this technology possible, and we are seeing it being used in an increasing number of applications - from Facebook, where it is used to identify individuals in posted photos, to marketing companies that embed face-ID enabled cameras into billboards to deliver targeted ads.

**Why use it?**

Common to many facial recognition applications is one underlying task - being able to automate the process of image review, and to search much larger data sets than a human could practically do on their own; or else to perform image analysis at much greater speed than human review allows. That's largely why this technology is of interest to potential users, but there are other possible uses as well. In government, the various applications range from suspect identification for law enforcement, to fraud prevention in human services.

As this technology is being quickly operationalized, we believe that the legislature should be proactive about evaluating the impact of this technology, as well as regulating its use. So let's quickly look at some of the policy questions the legislature will likely face regarding facial recognition technology:

**Investigative image matching**

As I've mentioned, one possible law enforcement application of facial recognition would be to automate image matching in order to identify images of crime suspects captured by photos or video.

The regulatory issues surrounding this application will largely turn on two questions: How accurate are the systems that are being used? And what processes will be triggered by a positive image match in a facial recognition system?

The relative accuracy of facial recognition systems has been a major point of discussion in recent years. Various academic studies, for instance, have raised questions about system accuracy and reliability. So, to the degree that system outcomes are relied upon to trigger specific outcomes - such as arrests - that will be an area of discussion, and possible regulation. At the federal level, for instance, the Government Accountability Office (GAO) has recommended "best practices" to the FBI for acquiring facial recognition systems.

The other part of the discussion involves the consequences that result from a positive image match. Will departments rely solely on a positive image match in a facial recognition system for probable cause to arrest? Or will departments use officer review to confirm an image match for the purpose of probable cause determinations? Another set of questions involves whether this will be a matter of individual departmental policy, or whether state regulation is required.

**What databases will be reviewed?**

As facial recognition relies upon a database of known images to try to identify an unknown image, questions naturally arise over which databases will be permissible to review - and under what standards. Since the state maintains some large photographic databases, which of these databases will be allowed to be searched?

For an example, will the state's drivers' license photo database be utilized as a facial recognition data set? Right now, the data classification of drivers' license photos maintained by DPS is "private", and Minn. Stat. § 171.07 places some parameters around which government entities can access that data — entities which include criminal justice agencies, coroners, and public defenders. Areas to explore include whether any of these entities have considered using this drivers' license data set in conjunction with facial recognition technology, and under what circumstances. Answers to those questions may drive the development of policy around how data sets can be used in connection with face ID technology, and the parameters that would be placed around government agency image-sharing.

As a side note, I would highlight the fact that some drivers' license data-sharing provisions are already in place in Minn Stat. § 171.12 for non-REAL ID compliant licenses. These provisions bar the sharing of non-REAL ID drivers license data with entities outside the state of Minnesota, and could reasonably be interpreted to prohibit the inclusion of those images in federal facial recognition databases — but that issue should be examined in more detail.

**Real-time surveillance**

The most controversial use of facial recognition technology is the integration of facial recognition software into government video camera feeds, thus enabling real-time identification and tracking of individuals who appear on camera. Because of this capability, there exists the potential to create a database of where everyone in a particular urban area has appeared in public, at almost any given point in time.

The potential for the mis-use of such systems is what sparks concerns about their implementation. These real-time surveillance processes are in wide use by the

Chinese government, for instance, which has proactively built up a domestic surveillance infrastructure - with extensive camera networks integrated with facial recognition - aimed specifically at population tracking and control. This is very much on the minds of the pro-democracy protesters in Hong Kong at present, as one can see from news footage of demonstrators toppling surveillance camera towers, and appearing in public wearing masks.

The prevalence of municipal video cameras in the Twin Cities metropolitan area raises questions about whether real-time tracking software could be installed into this existing network. You can look to a story that Minnpost did a couple years ago, in which they mapped out the areas of Minneapolis and Saint Paul that are currently monitored by municipal surveillance cameras. From the story, you can see that the bulk of downtown Minneapolis and Saint Paul are monitored - and the Minnpost review only included municipal cameras. Now that such infrastructure exists, questions naturally arise about what other technologies might be piggy-backed on the existing camera network, and what kind of individual-specific databases could be compiled. These kinds of surveillance database questions - specifically around location information connected to license plates - were first visited by the legislature in the debate over automated license plate readers that began in 2014. Representative Scott carried the House ALPR regulatory bill that is now codified at § 13.824.

The Constitution's Fourth Amendment is also involved in this matter, with questions arising about whether a comprehensive, real-time, face-ID surveillance system would be constitutional. Under existing search and seizure case law, items and persons in publicly accessible areas generally fall under the "plain view" doctrine. However, the government has not had the ability to view all of a public area at all times until recently—- and the question of whether this kind of comprehensive, enhanced surveillance constitutes a search under the Fourth Amendment then arises. A concurrence in a 2012 U.S. Supreme Court case (*United States v. Jone*s) indicates that the court is thinking about this issue of how far the government can go in surveilling the ongoing movements of individuals, for instance.

There are other matters that we'd urge the legislature to look into as well, including the government's use of software to make automated so-called "decisions" - and the transparency issues that flow from the use of such software … as well as the private sector building up image data banks, and then licensing them to government entities for integration into facial recognition programs.