

THE EXTRA NEWS

ALL ABOUT THE BIG TECHNO WORLD WE LIVE IN

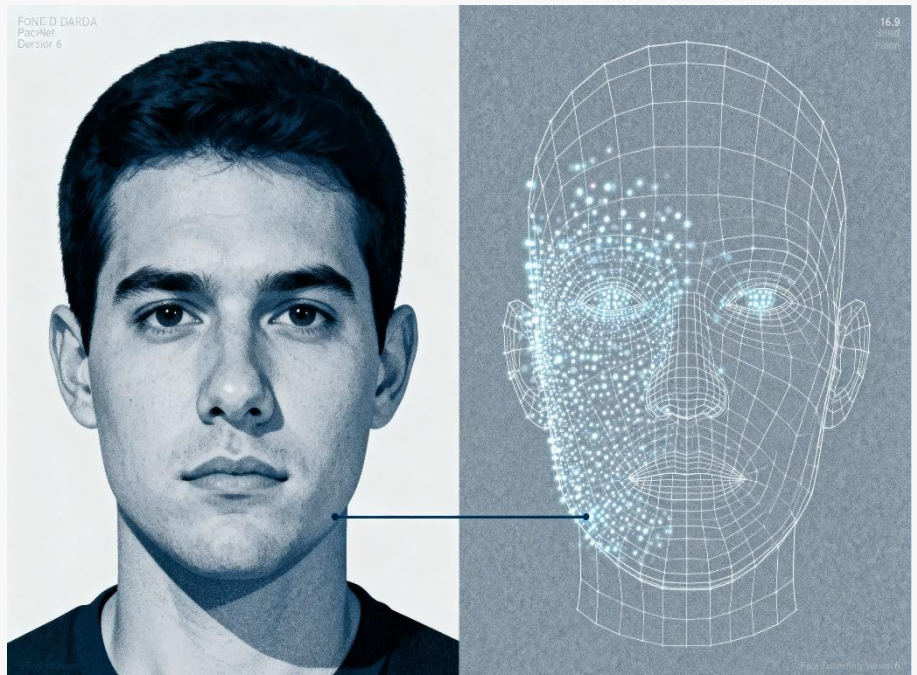
EXCLUSIVE AI NEWS

Deep Learning Spotlight The DMV's Silent Fraud Cop

By Michael Nobles,
Deep Learning Reporter
Extra News — October 28, 2025

Bismarck, North Dakota — Picture a typical Tuesday afternoon in Bismarck, where the gray DMV waiting room buzzes with impatience. A man in a Carhartt jacket slid a birth certificate across the counter. Name: John Miller. Birthdate: 1987. The clerk entered his information into the system, told him to “say cheese,” and took his photograph. Approximately 2.3 seconds after the photo was taken, the screen flashed red, displaying an alert message: “Mr. Miller” was in the system—with a different name, a different photograph, but the same cheek bones. North Dakota’s facial recognition system had detected another individual attempting to commit identity theft. There were no sirens, no handcuffs, simply a discreet alert and a polite request from the nice clerk for additional identification.

This is the power of North Dakota’s Facial Recognition System, which has been utilized by the state as part of the motor vehicle licensing



process since at least 2012. In researching this story, I reviewed North Dakota Department of Transportation (NDDOT) reports, academic studies, and the original reporting on this facial recognition system to learn how it operates—and whether it is worth the potential cost to privacy rights.

WHAT’S IT CALLED?

The official title of the application is the North Dakota Driver’s License Facial Recognition System, a biometric identification system incorporated into North Dakota’s motor vehicle licensing process. Although similar to commercial facial recognition systems—such as those developed by Clearview AI—this system is a custom-developed application built and

Deep Learning Spotlight: The DMV’s Silent Fraud Cop

North Dakota’s DMV doesn’t chase crooks—it stops them at the counter. Since 2012, every license photo is checked in real time against 500,000+ records.



Deep Learning Spotlight, continued

maintained by the State of North Dakota, commonly referred to as “ND Facial Recognition for DL/ID issuance.” As reported in NDDOT internal documents and the original public reporting on this issue—a May 7, 2012, *Grand Forks Herald* article—the system was identified and its functionality detailed before it was publicly disclosed. The article explained that the system takes a photograph of each applicant during the driver’s license application process and sends the image directly to a central server for comparison to ensure zero duplication. According to the article, the facial recognition system had already prevented “several” instances of fraudulent driver’s license applications. Unlike modern commercial facial recognition systems, this one was custom-designed for use within DMV workflows by the State of North Dakota, either internally or with minimal outside assistance, in contrast to large-scale commercial vendors (North Dakota Department of Transportation, n.d.; *Grand Forks Herald*, 2012).

HOW DOES IT WORK IN THE REAL WORLD?

Each of the 33 driver license issuing offices within the state requires applicants to remove all hats, sunglasses, and other items that may obstruct their face before a standardized, high-resolution photograph is taken in a controlled, lit environment. The photograph is then instantly transmitted to a central server and compared in real time to 500,000+ photographs in the system—representing simple ID cardholders and the state’s licensed driving population. The facial recognition system utilizes one-to-one (1:1) comparisons, rather than mass surveillance techniques. When the similarity between the photographed applicant and any existing record within the system hits a predetermined threshold (generally between 90–95%), the examiner’s computer terminal displays an alert notification. At that point, the DMV clerk will request further identification from the applicant, check the applicant’s fingerprints, or research any previous history involving the applicant.

The facial recognition system is for the sole purpose of identifying duplicate individuals and preventing unauthorized access to driver’s licenses and/or state ID cards—not for monitoring parking lots or crowds. Reportedly, the system has already detected

numerous fraud attempts using duplicate identities. Additionally, as reported in 2012, today the facial recognition system currently handles over one million transactions per year—from renewal applications to new driver’s license issuances—and continues to remain the primary method of verifying an individual’s true identity when applying for a driver’s license or state ID card in North Dakota (North Dakota Department of Transportation, 2024; *Grand Forks Herald*, 2012).



WHAT TYPE OF AI IS BEING USED?

While the NDDOT has not publicly identified the vendor tasked with the development of its facial recognition system, the architecture is likely built upon convolutional neural networks (CNNs), the core of most modern facial recognition systems. The top candidate models include FaceNet (Google, 2015) and ArcFace (InsightFace). These models convert facial images into compact vectors, typically ranging from 128 to 512 dimensions, which serve as mathematical signatures for the recognition process. The training methodology likely utilizes triplet loss to ensure that images of the same person are clustered close together in the same vector space regardless of differences in age (i.e., 16 vs. 60), lighting, or location (e.g., fluorescent lighting in the DMV versus harsh sunlight on the prairie). Lower-level layers in the CNNs identify edges, textures, and contours (for example, jawline curves), while upper-layer layers capture the overall structure of a face.

North Dakota may also utilize transfer learning—using a pre-trained model and then adapting it to the unique demographics of its residents (Native Americans, immigrants, etc.) and variable lighting conditions found in its various branches. Benchmarks have shown that laboratory-based facial recognition models utilizing CNNs achieve an accuracy rating of 99.63% on the *Labeled Faces in the Wild* dataset. Moreover, in real-world applications of the facial recognition system used in the DMV, results have similarly demonstrated effectiveness (Wang & Deng, 2021; Schroff et al., 2015).



Deep Learning Spotlight, CONTINUED

Bias can misidentify darker skin. A breach risks 500,000 faces. Most drivers never see the fine print about indefinite storage.

WHAT COULD GO WRONG?

Two major concerns with the facial recognition system include bias and privacy issues. According to a 2019 study published by the National Institute of Standards and Technology (NIST) entitled the *Face Recognition Vendor Test*, error rates for Black females were 30 times greater than those of white males, particularly in older or less-than-ideal systems (Grother et al., 2019). Furthermore, a false positive could incorrectly deny an eligible applicant a valid driver's license; whereas a false negative would allow a fraudulent applicant to obtain a valid driver's license.

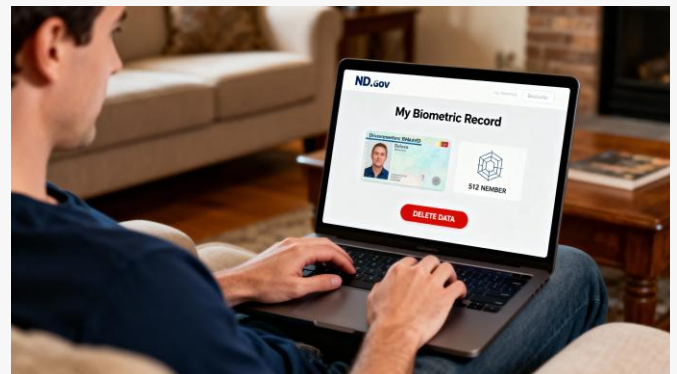
The second concern involves privacy, given that there's a high likelihood of over 500,000 biometric records contained in a single centralized North Dakota database. A single breach of the facial recognition database could potentially expose the lifelong identifiers of an individual—which is a tad more difficult to alter than a password. Lastly, consent is the final concern, as the mention of “biometric comparison” is buried in the legal jargon of the license application, and many applicants are unaware that their facial characteristics are captured and stored indefinitely, being compared to every subsequent renewal image of their driver's license.



HOW ARE THEY FIXING IT?

The NDDOT conducts an annual audit of its system using NIST-compliant bias testing and continually trains its system using many different demographics from North Dakota—including rural farmers, urban students, tribal members, and recently immigrated persons. All original photographs are converted into unreadable strings using a one-way hash function with

AES-256 encryption and are then placed in a secure database behind two layers of security during transmission between offices. Each office is supposed to post a notice that says: *“Your photograph is used to identify potentially fraudulent activity. Please ask us about how we protect your personal information.”* Unfortunately, I have not yet had the opportunity to verify this sign. When there has been a false positive (i.e., identical twin or doppelgänger), the applicant may request complete removal of all biometric data from the state's database using a formal procedure (North Dakota Department of Transportation, 2024).



WHAT SHOULD COME NEXT?

Provide the clerks at the DMV with some type of visual heatmap showing exactly where on the face (eyes, nose, jaw) the computer is flagging a possible identity match. Implement federated learning so that the individual camera systems at each DMV location would learn from and train their own local copy of the model—and never send any raw photographs off-site. Allow citizens to log into a portal where they can access and delete their biometric data if they wish to opt out. Some people have even suggested adding iris scanning and/or voice recognition technology for those who may not have the same facial features and could potentially be identified incorrectly. I, for one, am not one of those people.

The North Dakota DMV is not a sci-fi movie. It's a 13-year-old piece of technology that, to this day, continues to help the DMV stop individuals from attempting to commit identity theft/fraud through their locations—and proves AI can help protect identity while also protecting privacy, as long as someone continues to watch the watchers.

REFERENCES

- Grand Forks Herald. (2012, May 7). North Dakota using facial-recognition software when taking driver's license photos. <https://www.grandforksherald.com/newsmd/north-dakota-using-facial-recognition-software-when-taking-drivers-license-photos>
- Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) part 3: Demographic effects. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8280>
- NightCafe Studio. (2025). *AI-generated images for "Deep Learning Spotlight: The DMV's Silent Cop"* [Digital images]. <https://nightcafe.studio>
- North Dakota Department of Transportation. (2024). Transportation handbook: Annual vehicle registration statistics. <https://www.dot.nd.gov/sites/www/files/documents/Motor%20Vehicle%20Services/Transportation-Handbook-Annual-Vehicle-Reg-2024.pdf>
- North Dakota Department of Transportation. (n.d.). Driver license. <https://www.dot.nd.gov/driver/driver-license>
- Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 815–823. <https://doi.org/10.1109/CVPR.2015.7298682>
- Wang, M., & Deng, W. (2021). Deep face recognition: A survey. Neurocomputing, 429, 215–244. <https://doi.org/10.1016/j.neucom.2020.11.059>

OUTLINE

- **Introduction**
 - Hook: DMV camera catches fraud before the card prints.
 - Thesis: North Dakota's facial recognition system, live since at least 2012.
 - Approach: Cite 2012 Grand Forks Herald article + NDDOT data.
- **Application Name**
 - Official: North Dakota Driver's License Facial Recognition System.
 - Custom-built, not commercial; anti-fraud focus.
 - Sources: 2012 Herald, NDDOT site.
- **Usage**
 - Process: Photo → real-time 1:1 match → clerk alert.
 - Scale: 500k+ records, all 33 sites, 1M+ transactions/year.
 - Sources: 2012 Herald, NDDOT 2024.
- **Model**
 - CNN-based (FaceNet/ArcFace likely).
 - Triplet loss, embeddings, transfer learning.
 - Sources: Schroff 2015, Wang & Deng 2021.
- **Ethical Risks**
 - Bias (NIST), privacy (breach risk), consent (fine print).
 - Source: NIST 2019.
- **Fixes**
 - Audits, hashing, signage, deletion.
 - Source: NDDOT 2024.
- **Suggestions**
 - Heatmaps, federated learning, citizen portal.
- **Conclusion**
 - Old tech, still sharp — with guardrails.