FACIAL RECOGNITION AI: ALASKA IS AN IDEAL FORUM FOR INTRODUCING REGULATION

*Sarah Edwards**

ABSTRACT

As artificial intelligence becomes increasingly commonplace, we are all exposed to shockingly dystopian forms of surveillance. This Note details the unique danger of facial recognition technologies powered by artificial intelligence. First, this Note examines the rise of facial recognition technologies in both the public and the private sector. It illustrates this phenomenon by highlighting a few key players in both the development and implementation of facial recognition. Second, it proceeds by examining the current privacy landscape in Alaska. Alaska's unique focus on privacy rights makes the State a promising forum for regulation. Finally, it provides possible statutory and judicial solutions to stop the spread of these technologies and secure the privacy rights of Alaskan citizens and visitors.

I. INTRODUCTION

Surveillance has become an inescapable part of life in recent years. Most citizens are likely aware that most public spaces, especially stores, have security cameras. Many of us have grown accustomed to near constant video surveillance in public. But these cameras often do more than just film. Assisted by artificial intelligence, the footage is used to create scans of faces and catalogue unique biological identifiers.[1] These

* J.D. Candidate, Duke University School of Law, 2025; B.A., Comparative Religion and Psychology, Miami University, 2022. Thank you so much to everyone on the *Alaska Law Review* team for their help during the editing process. I would also like to thank Professor Sarah Baker and my Scholarly Writing classmates for their feedback and support during the writing process. Finally, I would like to thank my family and friends for their unwavering support, especially my parents, who have made everything possible for me.

1. *See* Elena Beretta & Nasir Muftić, *Facial Recognition: An Introduction*, INS. FOR INTERNET & THE JUST SOC'Y (Aug. 27, 2021), https://www.internetjustsociety.org/cosmonaut/facial-recognition-an-introduction (describing facial recognition artificial intelligence as a "biometric technique to uniquely identify a person by comparing and analyzing patterns

traits, such as the width between the eyes, or the angle from eye to nose,[2] are scanned against vast databases of facial images.[3] Those with access to the footage can click on a face and immediately access other images of the individual on the internet. These images contain other identifying information, such as the individual's name, hometown, and place of employment. In an instant, the filmed individual loses all privacy.

As dystopian as this sounds, use of facial recognition technology has become nearly ubiquitous.[4] It is currently used by an ever-growing number of government departments, law enforcement agencies, schools, and private corporations.[5] Widespread use of these technologies endangers privacy rights.[6] Despite the dangers, there currently exists no state or federal ban on untargeted facial recognition.[7]

Widespread use of facial recognition technologies threatens to permanently erode privacy. Regulation is needed across the country, but currently the most successful attempts at regulating the use of these technologies have been at the state level.[8] Because of Alaska's unique

based on their 'facial contours.'").

2. *Id.*

3. *See id.* ("Modern multinational companies have enormous power due to the vast amounts of data in their control, backed up by supreme algorithms and world-class scientists and experts.").

4. Rebecca Heilweil, *From Macy's to Albertson's, Facial Recognition is Already Everywhere,* VOX (July 19, 2021), https://www.vox.com/2021/7/15/22577876/macys-fight-for-the-future-facial-recognition-artificial-intelligence-stores.

5. *See id.* (noting that "the reach of facial recognition goes far beyond law enforcement and into the private, commercial storefronts we regularly visit.").

6. *See* Nigel Jones, *10 Problems with Facial Recognition,* THE PRIVACY COMPLIANCE HUB (Aug., 2021) https://www.privacycompliancehub.com/gdpr-resources/10-reasons-to-be-concerned-about-facial-recognition-technology/ (listing several of the most pressing concerns presented by facial recognition AI, including lack of consent, bias, and inaccuracies. Jones also writes that facial recognition "has real implications for fundamental human rights, including the right to protest, and the right to a private life.").

7. *See* Heilweil, *supra* note 4 ("One of the main challenges is that facial recognition is mostly unregulated, and many current efforts to rein in the technology primarily focus on its use by government and law enforcement." The author further notes that the dangers of facial recognition AI are felt acutely in remote areas because "[c]ustomers living in areas where there are few options for stores can end up being coerced into accepting the technology."); *see also* Jake Laperruque, *Limiting Face Recognition Surveillance: Progress and Paths Forward*, CTR. FOR DEMOCRACY AND TECH. (Aug. 23, 2022), https://cdt.org/insights/limiting-face-recognition-surveillance-progress-and-paths-forward ("Untargeted face recognition – in which, rather than scanning and identifying a single target, a system identifies all individuals in a video feed – is the most frightening use of this technology. . . Currently no states have a ban on untargeted scanning.").

8. *See* Carolina Rabinowicz, *Approaches to Regulating Government Use of Facial Recognition Technology,* HARV. J. OF L. AND TECH. (May 4, 2023), https://jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-

focus on privacy[9], the state presents an ideal forum for implementing meaningful regulation. In fact, Alaska has already implemented groundbreaking regulation of facial recognition technology at the municipal level.[10] But state-wide intervention remains immediately necessary, as corporations in Alaska seek to expand their facial recognition capabilities.[11] The ubiquity of facial recognition technology creates a pressing danger, and Alaska can curb its usage in both the public and private sectors.

Part II of this Note gives an overview of facial recognition AI and its use by private and public entities. Part III provides an overview of the privacy landscape in Alaska, highlighting a trailblazing municipal ordinance and a recent case with important ramifications for privacy rights. It argues that challenges to government use of facial recognition are likely to succeed in Alaska state courts based on judicial precedents and other privacy protections already in place. Finally, Part IV highlights a successful statutory solution and proposes that Alaska adopt similar legislation.

II. ARTIFICIAL INTELLIGENCE AND ITS APPLICATION TO FACIAL RECOGNITION

A. An Overview of Artificial Intelligence

Consider the above example of walking into a store and having your facial features scanned and catalogued. These technologies are powered by artificial intelligence. Artificial intelligence is "a system's ability to

of-facial-recognition-technology (explaining that "the federal government has not yet made progress on passing a FRT or biometric data bill"). A few federal proposals have been made, but none have been successful. It is not entirely clear why none of the federal proposals have succeeded, especially as the issue continues to grow in popularity. Passing federal regulation would "likely increase public confidence in the U.S. government's respect for citizen privacy." And "[t]he federal government also has access to much more data with a broader scope than individual states, meaning it can make more accurate decisions about whether a technology is discriminatory than a state with a narrower view and more limited resources." Despite these benefits, most successful regulation remains at the state level, thus this Note will focus on state level intervention in Alaska.

9. *See* ALASKA CONST. art. I, § 22.

10. *See e.g.* Anchorage, Alaska, Ordinance No. 2023-35-(S-1) (Apr. 18, 2023) (amending the Anchorage Municipal Code Ch. 3.102).

11. *See Alaska Airlines Announces Next Step of Biometric Strategy with Passport Verification Before International Travel,* ALASKA AIRLINES (Aug. 29, 2023), https://investor.alaskaair.com/news-releases/news-release-details/alaska-airlines-announces-next-step-biometric-strategy-passport ("[W]e're transforming the airport experience and reimagining how guests get from the lobby to the boarding door – and the use of biometric identities is at the center of this vision.").

interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation."[12] Commonly, artificial intelligence models are fed data and then train themselves over time to "find patterns or make predictions."[13] Despite its relatively simple definition, experts often struggle to define the scope of artificial intelligence[14] Regardless, artificial intelligence is already ubiquitous in daily life.[15]

Many users may not even be aware that artificial intelligence is crucial to the functioning of their personal cellular device.[16] AI already powers many convenient tools, including iPhone features like Siri, Face ID, and the Calendar application.[17] For example, the iPhone camera and Photos application create a map of users' faces, and then categorize photos based on the faces found in them.[18] This allows users to search

12. Andreas Kaplan & Michael Haenlein, *Rulers of the World, Unite! The Challenges and Opportunities of Artificial Intelligence*, 63 BUS. HORIZONS JAN.–FEB. 2020, at 37–50; *see also Artificial Intelligence,* ENCYCLOPEDIA BRITTANICA (Mar. 13, 2024), https://www.britannica.com/technology/artificial-intelligence ("[A]rtificial intelligence, the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalize, or learn from past experience.").

13. Sara Brown, *Machine Learning, Explained,* MIT SLOAN SCHOOL IDEAS MADE TO MATTER (Apr. 21, 2021), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained (explaining how artificial intelligence systems operate and learn over time. The author further notes common concerns about "explainability, or the ability to be clear about what the machine learning models are doing and how they make decisions." This lack of transparency may compound other problems with models, such as bias or inaccuracies.).

14. *See* Kaplan & Haenlein, *supra* note 12 (describing three main reasons why experts struggle to define artificial intelligence).

15. *See generally* Andreas Kaplan & Michael Haenlein, *Siri, Siri in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence*, 62 BUS. HORIZONS 15–25 (2019) (finding that AI applications are already widely used in universities, corporations, and government).

16. *See* Evan Selleck, *How Apple is Already Using Machine Learning and AI in iOS*, APPLE INSIDER (Nov. 20, 2023), https://appleinsider.com/articles/23/09/02/how-apple-is-already-using-machine-learning-and-ai-in-ios (Despite Apple's heavy reliance on artificial intelligence in developing iPhone models and features, the company avoids statements about "artificial intelligence." Notably, the company refers to its artificial intelligence initiatives as "machine learning." And "[i]n 2023, Apple is using machine learning in just about every nook and cranny of iOS.").

17. *Id.*

18. *See id.* ("Apple introduced the TrueDepth camera and Face ID with the launch of the iPhone X. The hardware system can project 30,000 infrared dots to create a depth map of the user's face. The dot projection is paired with a 2D infrared scan as well. That information is stored on-device, and the iPhone uses machine learning and the DNN to parse every single scan of the user's face when they unlock their device.").

their photos for those containing a specific face.[19] The iPhone uses this technology to create curated videos, featuring photos of one specific person, or from one specific location.[20] Users can even unlock their iPhone and access personal information with just their face.[21]

Artificial intelligence has already revolutionized industries such as healthcare, agriculture, transportation, education, and security.[22] For example, in healthcare, artificial intelligence is increasingly used to classify medical images automatically.[23] Studies have shown that artificial intelligence is able to "meet or exceed the performance of human experts in image-based diagnoses" in a number of specialties.[24] As medical screening can be costly and time-prohibitive, its automation has the potential to save lives through early disease detection.[25]

Despite its revolutionary potential, reliance on artificial intelligence is not without risks,[26] and American attitudes about artificial intelligence reflect those risks.[27] Indeed, over half of Americans "feel more concerned than excited about the increased use of artificial intelligence."[28] Experts in the field have expressed concerns as well.[29] Many worry that increased use of AI will contribute to economic inequality, misinformation, and job displacement.[30] Some experts have even gone as far as to say that "[i]f AI

19. *Id.*
20. *Id.*
21. *Id.*
22. Bernard Marr, *15 Amazing Real-World Applications of AI Everyone Should Know About*, FORBES (May 10, 2023, 2:51 AM), https://www.forbes.com/sites/bernardmarr/2023/05/10/15-amazing-real-world-applications-of-ai-everyone-should-know-about/?sh=30f2132885e8.
23. *See* Junaid Bajwa, *Artificial Intelligence in Healthcare: Transforming the Practice of Medicine,* FUTURE HEALTHCARE J. July 2021, at 188–94.
24. *Id.* ("The automated classification of medical images is the leading AI application today.").
25. *Id.*
26. *See* Isabella Backman, *Eliminating Racial Bias in Health Care AI: Expert Panel Offers Guidelines,* YALE SCH. OF MED. (Dec. 21, 2023), https://medicine.yale.edu/news-article/eliminating-racial-bias-in-health-care-ai-expert-panel-offersguidelines. ("[H]ealth care algorithms that power AI may include bias against underrepresented communities and thus amplify existing racial inequality in medicine, according to a growing body of evidence.).
27. *See generally* Alec Tyson & Emma Kikuchi, *Growing Public Concern About the Role of Artificial Intelligence in Daily Life,* THE PEW RSCH. INST. (Aug. 28, 2023), https://www.pewresearch.org/short-reads/2023/08/28/growing-public-concern-about-the-role-of-artificial-intelligence-in-daily-life/.
28. *Id.* (Americans in this survey were especially concerned about the interaction between artificial intelligence and privacy. In fact, almost 60 percent of college graduates felt that artificial intelligence "hurts more than it helps" regarding "keeping people's personal information private." Fifty percent of adults with lower educational attainment felt the same.).
29. *See generally* Kaplan & Haenlein, *supra* note 12.
30. *See* Marr, *supra* note 22 (expanding upon risks presented by artificial

turns bad—really bad—the risk could be full extinction with 0% survival."[31]

The tracking and compilation of biometric information presents some of these risks. AI is already commonly used to identify and track biometric information,[32] which some AI technologies can use for facial recognition.[33] Such technology has the capacity to "uniquely identify a person by comparing and analyzing patterns based on their facial contours."[34] While different programs and algorithms exist, they typically follow the same general steps. First, a camera detects an image of a face.[35] Second, the facial recognition software analyzes the facial geometry of that face, including features such as the distance between the eyes, the shape of the cheekbones, and the depth of the eye sockets.[36] Third, the program converts the facial geometry of the face into data known as a "faceprint," which is unique to every person.[37] Faceprint information is then stored as numerical code and compared to the program's faceprint database for potential matches.[38]

While the widespread usage of this technology is a recent development, facial recognition AI is not new. In fact, scientists developed rudimentary forms of facial recognition technology as early as the 1960s.[39] Since then, the technology has grown increasingly complex.

---

intelligence).

31. Kaplan & Haenlein, *supra* note 12.

32. *See* Beretta & Muftić, *supra* note 1 ("In fact, facial recognition systems can be used to identify people in photos, videos, or in real time."). Biometrics are defined as "unique physical characteristics . . . that can be used for automated recognition." *Biometrics,* DEP'T OF HOMELAND SECURITY (May 5, 2023), https://www.dhs.gov/biometrics [hereinafter *Biometrics*]. Examples of biometrics include voice recognition, fingerprints, and scans of unique physical identifiers such as retinas, irises, or facial contours. *Id.*

33. *See* Aleix M. Martinez, *Face Recognition, Overview,* ENCYCLOPEDIA OF BIOMETRICS (defining facial recognition as "the science which involves the understanding of how the faces are recognized by biological systems and how this can be emulated by computer systems."); *see also History of NIJ Support for Face Recognition Technology*, NAT'L INSTS. OF JUST. (March 5, 2020) https://nij.ojp.gov/topics/articles/history-nij-support-face-recognition-technology ("Face recognition technology is a potent, practical application of artificial intelligence.").

34. Beretta & Muftić, *supra* note 1.

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *See* Shaun Raviv, *The Secret History of Facial Recognition*, WIRED (Jan. 21, 2020, 6:00 AM), https://www.wired.com/story/secret-history-facial-recognition/ (detailing early facial recognition research by Woody Bledsoe in the 1960's. For years, Bledsoe's company contracted with the CIA who funded much of their research. As early as 1965, Bledsoe's company was able to train early computers to recognize and identify ten faces. By 1967, Bledsoe contracted with

In the early 2010s, a number of large tech companies turned their attention to developing facial recognition software.[40] As early as 2011, an engineer from Google "revealed he had been working on a tool to Google someone's face and bring up other online photos of them."[41] The chairman of Google, Eric Schmidt, in referring to the company's project, said, "[a]s far as I know, it's the only [facial recognition] technology that Google built and, after looking at it, we decided to stop."[42] Although Google ultimately decided not to release this tool,[43] other tech companies have continued developing and releasing exactly the kind of technology that Google felt was too dangerous for public use.[44]

---

the CIA to "help law enforcement agencies quickly sift through databases of mug shots and portraits, looking for matches.").

40. Kashmir Hill, *The Technology Facebook and Google Didn't Dare Release*, N.Y. TIMES (Sept. 9, 2023) [hereinafter *Didn't Dare Release*], https://www.nytimes.com/2023/09/09/technology/google-facebook-facial-recognition.html; *see also* Kashmir Hill & Ryan Mac, *Facebook, Citing Societal Concerns, Plans to Shut Down Facial Recognition System*, N.Y. TIMES (June 22, 2023), https://www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.html (noting that the company formerly known as Facebook adopted a platform-wide facial recognition technology in 2010 to "automatically identif[y] people who appeared in users' digital photo albums and suggested users 'tag' them all with a click, linking their accounts to the images." Through its use of this technology, Facebook created one of the largest databases of digital images in the world. In 2019, the Federal Trade Commission fined the company $5 billion for privacy complaints, and in 2020 the company agreed to pay $650 million in a state law settlement for biometric privacy violations. In 2021, following these lawsuits, congressional hearings, and regulatory inquiries, Facebook announced that it would discontinue its use of the technology. The company pledged to delete "more than one billion facial recognition templates, which are digital scans of facial features." Despite this promise, Facebook opted not to get rid of the software behind their facial recognition program, a computer algorithm called DeepFace.").

41. *See Didn't Dare Release*, *supra* note 40.

42. *Id.* (Despite not releasing such a tool, large tech companies continued to use facial recognition technology in other ways, such as "a security tool to unlock a smartphone, a more efficient way to tag known friends in photos and an organizational tool to categorize smartphone photos by the faces of the people in them.")

43. *Id.*

44. *Id.* ("Clearview AI and PimEyes have pushed the boundaries of what the public thought was possible by releasing face search engines paired with millions of photos from the public web (PimEyes) or even billions (Clearview). . . What these start-ups had done wasn't a technological breakthrough; it was an ethical one. Tech giants had developed the ability to recognize unknown people's faces years earlier, but had chosen to hold the technology back, deciding that the most extreme version – putting a name to a stranger's face – was too dangerous to make widely available.").

B. Clearview AI as an Example of a Facial Recognition Giant

Despite the risks, smaller startups continued developing facial recognition technology, including a company called Clearview AI.[45] Founded in 2017, Clearview took advantage of large tech companies' hesitance to develop and release facial recognition databases to develop its own.[46] To do so, Clearview sourced billions of images from publicly available websites, such as Instagram, Facebook, and Venmo.[47] To date, Clearview has amassed over 30 billion facial images.[48] Users can upload an image, and Clearview "processes the image and returns links to publicly available images that contain faces similar to the person pictured in the image."[49] According to Clearview, its algorithm will "take into account age progression, variations in poses and positions, changes in facial hair, and many visual conditions and [*sic*] to perform at 99% or better across all demographic groups on key tests."[50]

In 2020, leaked documents revealed Clearview's customer base, showing that Clearview AI's use was much more pervasive than previously estimated.[51] At the time of the leak, Clearview's database had

45. *Company Overview*, CLEARVIEW AI, https://www.clearview.ai/overview (last visited Feb. 3, 2024) [hereinafter *Clearview*] ("Clearview AI is a privately-owned, U.S. based company, dedicated to innovating and providing the most cutting-edge technology to law enforcement to investigate crimes, enhance public safety and provide justice to victims.").

46. *See id.* ("[W]e developed a revolutionary, web-based intelligence platform for law enforcement to use as a tool to help generate high-quality investigative leads. Our platform, powered by facial recognition technology, includes the largest known database of 30+ billion facial images sourced from public-only web sources, including news media, mugshot websites, public social media, and other open sources."); *see also Didn't Dare Release*, *supra* note 40 (describing Clearview's founder Hoan Ton-That's "quest to create a groundbreaking and more lucrative app." Mr. Ton-That described various free online resources he used to create the data base and algorithm, such as a 'face-recognition library' called OpenFace. Mr. Ton-That is quoted as saying "I couldn't have done it if I had to build it from scratch, . . . I was standing on the shoulders of giants.')

47. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020) [hereinafter *Secretive Company*], https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

48. *How We Store and Search 30 Billion Faces*, CLEARVIEW AI, https://www.clearview.ai/post/how-we-store-and-search-30-billion-faces (last visited Feb. 3, 2024) ("The Clearview AI platform has evolved significantly over the past few years, with our database growing from a few million face images to an astounding 30 billion today.").

49. *What We Do and How Does It Work?*, CLEARVIEW AI, https://www.clearview.ai/principles (last visited Feb. 3, 2024).

50. *Id.*

51. Ryan Mac, *Clearview's Facial Recognition App Has Been Used by the Justice Department, ICE, Macy's, Walmart, and the NBA*, BUZZFEED (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-

been accessed by "people in more than 2,200 law enforcement departments, government agencies, and companies across 27 countries."[52] Many of these searches were completed without a formal contract, but rather through free trial subscriptions.[53] Law enforcement agencies made up a significant swath of Clearview's clientele,[54] including many that had already run thousands of searches at the time of the leak.[55] Over fifty educational institutions were using Clearview, including two high schools.[56] And over 200 private companies took advantage of the service,[57] including Madison Square Garden, the NBA, Coinbase, Equinox, Walmart, Best Buy, Rite Aid, Kohl's, Verizon, Las Vegas Sands, and forty-six separate financial institutions.[58]

But following a groundbreaking settlement in Illinois in 2020, Clearview was enjoined from licensing its services to private entities and individuals.[59] As further discussed in Part IV, the ACLU successfully sued Clearview under a private right of action created by a trailblazing Illinois state regulation because of its failure to implement even basic oversight standards.[60] However, Clearview is far from the only company offering a

law-enforcement.

52. *Id.* While many users took advantage of free trial subscriptions, various law enforcement offices paid for subscriptions. For example, the New York State police department paid $15,000 for Clearview licenses and the Atlanta Police Department paid $6,000. *Id.*

53. *See id.* ("Clearview's propensity to hand out free trials to officers using police department or governmental email addresses has sometimes created situations in which law enforcement agencies appear to have no idea the tool is being used by their employees. While the nation's largest police department, the NYPD, previously denied it had any formal relationship with Clearview, the document shows that officers there have run more than 11,000 searches, the most of any entity on the document. More than 30 officers have Clearview accounts, according to the log. An NYPD spokesperson told BuzzFeed News that while it does not have any contract or agreement with Clearview, its established practices did not authorize the use of services such as Clearview AI nor did they specifically prohibit it.")

54. *Id.* ("Beyond the federal government, Clearview AI's free trials have inspired facial recognition usage in hundreds of regional, state, county, and local law enforcement agencies.").

55. *Id.* ("The Miami Police Department, for example, had run over 3,000 Clearview searches, according to the documents. The San Mateo County Sherriff's Office has run about 2,000 searches, as has the Philadelphia Police Department. The Indiana State Police, identified in the startup's documents as a paying agency, has run more than 5,700 scans.").

56. *Id.*

57. *Id.*

58. *Id.*

59. Summary of *ACLU v. Clearview*, ACLU (May 11, 2022), https://www.aclu.org/cases/aclu-v-clearview-ai (summarizing *ACLU v. Clearview AI* (*Clearview II*), No. 2020 CH 04353, U.S. LEXIS 2887 (Ill. Cir. Ct. May 11, 2022)).

60. *Id.* ("The lawsuit was filed in Illinois state court in Chicago, after the New

facial recognition database of this kind.[61] As an increasing number of companies develop their own facial recognition technology, without comprehensive regulation, private entities will use it at increasing rates.[62]

C. Use of Facial Recognition AI by Private Entities

Without meaningful guardrails on the development and sale of facial recognition technologies, its use has expanded beyond government and law enforcement. It is now commonplace for private entities, such as banks, airlines, and retailers, to employ facial recognition tools.[63] Businesses tout their use of facial recognition as a tool to improve consumer safety, security, and convenience.[64]

But misuse is already occurring. Consider, for example, the plight of Kelly Conlon.[65] In 2021, she entered Radio City Music Hall to accompany her daughter's Girl Scout Troop to the Rockettes' "Christmas

York Times revealed in January 2020 that Clearview was building a secretive tracking and surveillance tool using biometric identifiers. Face recognition technology has helped Clearview capture more than three billion faceprints, and counting, from images available online.").

61. *See The Best Facial Recognition Datasets of 2022*, TWINE AI (July 8, 2022), https://www.twine.net/blog/facial-recognition-datasets/ (listing the blog's choices for best facial recognition datasets of the year, including platforms such as Flickr-Faces-HQ Dataset, Tufts Face Dataset, Labeled Faces in the Wild Dataset, UTKFace Dataset, The Yale Face Dataset, Face Images with Marked Landmark Points Dataset, and Google Facial Expression Comparison Dataset.); *see also* Thorin Klosowski, *Facial Recognition is Everywhere. Here's What We Can Do About It*, N.Y. TIMES (July 15, 2020), https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/ ("Clearview AI is an outlier only in that it has faced public scrutiny: Equally less ethical software companies exist – companies that will sell their software to local law enforcement, usually with no oversight or public scrutiny into where the photos come from or how the identification algorithms work.").

62. *See* Max Zahn, *Controversy Illuminates Rise of Facial Recognition in Private Sector*, ABC NEWS (Jan. 7, 2023), https://abcnews.go.com/Business/controversy-illuminates-rise-facial-recognition-private-sector/story?id=96116545 (quoting Meg Foster of Georgetown University's Center on Privacy and Technology, "[o]ver the last few years there has been a quiet surge in the use of facial recognition by private companies. . . . We've seen a huge rise in this technology").

63. *See generally id.*

64. *See id.* (quoting a spokesperson from Madison Square Garden Entertainment, "[f]acial recognition technology is a useful tool widely used throughout the country, including the sports and entertainment industry, retail locations, casinos and airports to protect the safety of the people that visit and work at those locations").

65. Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies*, N.Y. TIMES (Dec. 22, 2022), https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.

Spectacular."[66] But before she could enter, she was pulled away by security guards who informed her that she was on the venue's "attorney exclusion list."[67] Based on a scan of her face taken while she walked in, guards knew her name and her place of employment.[68] James Dolan, the chief executive for Madison Square Garden, had banned all lawyers working at any firm that has represented people suing Madison Square Garden Entertainment or any of its subsidiaries from the venue.[69] In order to enforce this ban, the venue uses facial recognition technology that "can identify hundreds of lawyers via profile photos on their firms' own websites, using an algorithm to instantaneously pore over images and suggest matches."[70] This algorithm identified Ms. Conlon, despite the fact that she does not practice in New York nor advise clients in cases against MSG Entertainment.[71]

This practice was widely criticized.[72] One commentator, Evan Greer, a digital rights activist, said of the ban: "We're talking about a powerful corporation's petty grievance, . . . But it's just really scary to think about the ways this technology could enable powerful individuals, companies, and institutions to target critics, business rivals, journalists, love interests – you name it."[73] And New York State Senator Brad Hoylman said: "Frankly, they owe it to New Yorkers to stop this type of bullying behavior, and allow every patron who wants to see a game or see a show

66. *Id*. Radio City Music Hall is owned by MSG Entertainment.

67. *Id*. (The article describes the plight of a number of other lawyers who have been targeted through this list. Another attorney, Alexis Majano, was kicked out of a Knicks game. Yet another attorney, Nicolette Landi, was denied entry to a Mariah Carey concert despite having purchased a ticket.)

68. *Id*.

69. *Id.* Ms. Conlon's firm, Davis, Saperstein, & Salomon, is representing a client in a personal injury case against one of MSG Entertainment's restaurants. *Id.*

70. *Id.*

71. *Id*.

72. *See e.g*. Manuela Lopez Restrepo, *She was Denied Entry to a Rockettes Show – Then the Facial Recognition Debate Ignited,* NPR (Jan. 21, 2023, 7:00 AM), https://www.npr.org/2023/01/21/1150289272/facial-recognition-technology-madison-square-garden-law-new-york ("The story has become a flashpoint in the debate around facial recognition technology. While proponents say it has the ability to keep people safer, critics counter that there is little support to this idea, and warn that unchecked use of the technology could have untold consequences."); *see also* Sarah Wallace, *MSG Doubles Down on Ban for Attorneys Suing It Amid Face Recognition Tech Scrutiny,* NBC N.Y. (Jan. 24, 2023, 10:34 AM) https://www.nbcnewyork.com/investigations/msg-doubles-down-on-ban-for-lawyers-suing-them-as-lawmakers-may-target-face-recognition/4064038/ (quoting attorney and Knicks season ticket holder Larry Hutcher, "We're New Yorkers, we're not gonna sit still, and see you act like the bully that you are, . . . [i]t's clear that everyone recognizes that Dolan has acted in an arbitrary and capricious manner, it is based in a mean-spirited and vindictive way.").

73. *See Madison Square Garden Uses Facial Recognition supra* note 65.

at Radio City the opportunity to do so."[74]

Real-time facial recognition by private entities allows businesses to identify and exclude anyone, and these programs are being rolled out despite their technical weaknesses. Facial recognition technologies have been shown to be far less effective at identifying people of color than white people.[75] Accuracy varies between demographics, "with the poorest accuracy consistently found in subjects who are female, Black, and between eighteen and thirty years old."[76] Different databases also have different levels of effectiveness.[77] These differences and inaccuracies have an outsized impact on minority communities.[78]

There is no way to opt out of most private facial recognition programs. If you enter a store that uses facial recognition software, your face is scanned upon entry without your knowledge or consent. Your picture is likely already in their database, sourced from the internet, again, without your knowledge or consent. If private corporations choose to sell this data, or if it is stolen, consumers have virtually no recourse.[79] Biometric identifiers used for facial recognition cannot be changed.[80]

Despite the risks of private corporations using facial recognition technology, its use continues to grow, even in Alaska. Citizens are not free

74. Wallace *supra* note 72.

75. *See* Alex Najibi, *Racial Discrimination in Facial Recognition Technology,* HARV. UNIV. GRADUATE SCH. OF ARTS AND SCIS. BLOG, SCI. POL'Y, SPECIAL ED.: SCI. POL'Y & SOC. JUST. (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

76. *Id.* ("Independent assessment by the National Institute of Standards and Technology (NIST) has confirmed these studies, finding that face recognition technologies across 189 algorithms are least accurate on women of color.").

77. *Id.*

78. *Id.* ("Surveillance is linked to behavioral changes including self-censorship and avoiding activism for fear of retribution; for example, face recognition was employed to monitor and identify Black Lives Matter protestors. The FBI has a long history of surveilling prominent Black activists and leaders to track and suppress their efforts. Additionally, continual surveillance induces fear and psychological harm, rendering subjects vulnerable to targeted abuses, as well as physical harm, by expanding systems of government oversight used to deny access to healthcare and welfare. In a criminal justice setting, face recognition technologies that are inherently biased in their accuracy can misidentify suspects, incarcerating innocent Black Americans.").

79. *See* Restrepo *supra* note 72 (quoting the executive director of the Surveillance Technology Oversight Project, Albert Fox Cahn, "[y]ou can change your name, you can change your social security number, you can change almost anything, but you can't change your face, . . . So if your biometric data is compromised once, it's compromised for life.").

80. *See Biometric Information Privacy Act (BIPA),* ACLU OF ILL., https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (last visited Feb. 4, 2024) ("Unlike a phone number, email address, or other password, biometric information can never be changed!").

from its reach even in remote areas of the state. For example, Alaska Airlines recently announced plans to implement facial recognition technology into their check-in process beginning in 2024.[81] The airline plans to implement a "biometric boarding pass,"[82] which would scan passengers' faces rather than a physical boarding pass or a digital barcode.[83] Alaska Airlines is just one example of the continued expansion of these invasive technologies. Unlike most, it is a use in which citizens would at least *know* that their biometrics are being scanned and tracked.

III. THE ALASKA PRIVACY LANDSCAPE

A. History

Privacy is paramount in Alaska, making it an ideal state to regulate invasive facial recognition technologies. Following the Alaska Supreme Court's decision in *Breese v. Smith*,[84] a special privacy amendment was added to the state constitution in 1972. Article I, Section 22 of the Alaska Constitution reads "[t]he right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section."[85]

Once the Alaska Constitution enshrined privacy as a constitutional right, state courts reviewed privacy infringements under a traditional strict scrutiny test.[86] In *Ravin v. State,* the Alaska Supreme Court held that "[i]f governmental restrictions interfere with the individual's right to privacy, we will require that the relationship between means and ends be not reasonable but close and substantial."[87] This is a high standard to

81. Lauren Leffer, *Alaska Airlines Kills the Check-in Kiosk, Brings in Face Scanners*, GIZMODO (Apr. 18, 2023) https://gizmodo.com/alaska-airlines-kills-check-in-kiosk-adds-face-scanners-1850347504.

82. Joe Kunzler, *Alaska Airlines Turns to Tech to Elevate the Passenger Experience*, SIMPLE FLYING (Mar. 25, 2022) https://simpleflying.com/alaska-airlines-technology-incubator/.

83. *Id.*

84. *See generally* Breese v. Smith, 501 P.2d 159, 175 (Alaska 1972).

85. ALASKA CONST. art. I § 22.

86. *See* Ravin v. State, 537 P.2d 494, 500–01 (Alaska 1975) (describing how the Alaska Constitution has an enumerated privacy right where the federal Constitution does not. Therefore, while federal cases must use privacy theories such as penumbras, Alaska state cases should subject infringements of the privacy right to strict scrutiny. For a state measure to survive strict scrutiny analysis, it must "be of a compelling nature and must be identifiable as flowing from some enumerated constitutional power." There is no defined "nature or exact amount of evidence necessary to establish the existence of a compelling state interest." Courts will examine the entire record of a case to make this determination. If a compelling interest is found, courts must then examine whether the means used by the measure have a close and substantial relationship to its desired end.).

87. *Id.* at 498.

meet,[88] and it underscores just how important privacy is to Alaska. In fact, Alaska is one of only ten states with an enumerated constitutional right to privacy.[89]

The Alaska judiciary has recognized that this unique enumeration creates a heightened expectation of privacy for Alaska citizens. In *State v. Planned Parenthood of Alaska*, the Court held that "[b]ecause th[e] right to privacy is explicit, its protections are necessarily more robust and 'broader in scope' than those of the implied federal right to privacy."[90]

B. *Doe v. Department of Public Safety* as a Case Illustration

Indeed, courts in Alaska have repeatedly recognized a robust right to privacy in a wide range of cases. For example, in *Doe v. Department of Public Safety*, the Alaska Supreme Court grappled with the privacy interests of sex offenders.[91] It examined whether requiring sex offenders to register through the Alaska Sexual Offender Registration Act (ASORA) constituted a substantive due process violation of the constitutional right to privacy.[92]

ASORA requires sex offenders in Alaska to "disclose their name, address, place of employment, date of birth, information about their conviction, aliases, driver's license number, information about the vehicles they have access to, any identifying physical features, anticipated address changes, electronic addresses, and information about psychological treatment received."[93] Registrants must submit to finger printing and photographing.[94] Additionally, registrants must re-register and update their information either quarterly or annually.[95]

But ASORA does more than collect this information. ASORA

88. *See id.* at 497 (quoting *Breese v. Smith*, "Once a fundamental right under the constitution of Alaska has been shown to be involved and it has been further shown that this constitutionally protected right has been impaired by governmental action, then the government must come forward and meet its substantial burden of establishing that the abridgement in question was justified by a compelling governmental interest." The opinion goes on to say that "[t]he law must be shown 'necessary, and not merely rationally related, to the accomplishment of a permissible state policy.'").

89. Larry W. Thomas, *Legal Issues Concerning Transit Agency Use of Electronic Consumer Data*, LEGAL RSCH. DIGEST, March 2017, at 36.

90. State v. Planned Parenthood of Alaska, 171 P.3d 577, 581 (Alaska 2007) (applying the strict scrutiny standard); *see also* State v. Planned Parenthood of Alaska, 35 P.3d 30, 39–40 (Alaska 2001) (holding that the robust privacy rights enjoyed by Alaskans extend to minors).

91. Doe v. Dep't of Pub. Safety, 444 P.3d 116, 119 (Alaska 2019).

92. *Id.*

93. *Id.* at 120.

94. *Id.*

95. *Id.*

requires the Alaska Department of Public Safety to "maintain a central registry of sex offenders that contains the information obtained under ASORA."[96] Through this registry, members of the public can view registrants' "names, aliases, dates of birth, addresses, photographs, physical descriptions, motor vehicle information, places of employment, public information about their convictions and sentences, and whether the offender is in compliance with ASORA or cannot be located."[97] Photographs of registrants are available alongside this information.[98]

A sex offender, using the pseudonym John Doe, argued that the demands of ASORA registration violated the due process clause of the Alaska Constitution.[99] He argued that registration infringed on a number of his constitutionally protected rights, notably his right to privacy.[100] Doe further contended that the law would not be able to survive strict scrutiny.[101] Even if the government could articulate a compelling state interest, he argued, they would fail the least restrictive means test.[102] ASORA did allow offenders opt out of the program, even for non-violent offenders or those who did not pose a risk to society.[103]

The court reasoned that a sex offense conviction is sensitive personal information.[104] Availability of offense details combined with personal identifying information may subject offenders to "community scorn and leave them vulnerable to harassment and economic and physical reprisals."[105] The court further expressed concerns about the accessibility of the information compiled through ASORA.[106] It reasoned that the history of the Alaska constitutional privacy amendment "suggests that the potential for computers to aggregate was one of the core reasons for its adoption."[107] Because Alaska was motivated to enshrine its privacy right based on fears surrounding government computers, this issue falls directly within the privacy right protected by the amendment.[108] The Alaska Supreme Court quoted the United States Supreme Court, writing that: "plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives,

96. *Id.*
97. *Id.*
98. *Id.*
99. *Id.* at 124.
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.* at 126.
105. *Id.* at 128.
106. *Id.* at 128–29.
107. *Id.* at 128.
108. *Id.*

and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[109]

The court held that sex offenders do have a legitimate privacy interest in keeping the details of their convictions and personal identifying information from dissemination to the public.[110] The court considered concerns about computerized compilations of personal information in its reasoning.[111] Having concluded that a legitimate privacy interest was at stake, the court held that "the right to privacy ensures that the state will not undertake such a program except where there is a compelling need, and only if the program is narrowly tailored to that need."[112]

C. Applying the Standards from Doe to a Challenge to Government Facial Recognition

As *Doe v. Department of Public Safety* illustrates, privacy is paramount in Alaska. Indeed, the Alaska Supreme Court held that the privacy amendment even protects sex offenders from the dangers of automated data collection.[113] So, one might infer that Alaska courts would choose to protect all citizens from unauthorized automated biometric data collection. Therefore, a challenge to government usage of facial recognition technology is likely to succeed in Alaska.

Courts would look to many of the principles underlying the Alaska Supreme Court's decision in *Doe* in a challenge of this kind. Lawmakers passed Article 1, Section 22 in response to concerns about computer aggregation of sensitive data.[114] Facial recognition databases, especially when used by law enforcement, employ such a system of data aggregation to match a face to its database.[115] Allowing the government

109. *Id.* at 129 (quoting U.S. Dept. of Just. v. Reporters Committee for Freedom of Press, 489 U.S. 749 (1989)).

110. *Id.* at 130 ("Our cases establish that the privacy clause protects against the release of information that can result in such harms in other contexts, and it is reasonable to expect that the privacy clause does so in the current context as well.").

111. *Id.* ("[T]he threats to personal privacy posed by government computer data compilations like the ASORA registry were a central concern underlying the enactment of the privacy clause in the Alaska [C]onstitution.")

112. *Id.*

113. *See id.* at 136.

114. *See id.* at 128 ("Leading up to the amendment's adoption there were 'persistent rumors that the Alaska State Troopers were compiling secret dossiers on Alaska citizens,' prompting 'considerable concern in the legislature in 1972 over the potential of systems like [the Alaska Justice Information System] for invasion into the privacy of individuals.'").

115. *See supra* Part II.A.

to collect and maintain biometric identifiers of individuals without their knowledge or consent harms the privacy interest protected by the Alaska Constitution because the collection of biometric data from personal photos is an affront to an individual's autonomy and decision-making.[116]

D. Other Alaska Privacy Statutes

Beyond Alaska's unique constitutional privacy protection, it also protects the privacy of its citizens through several other laws, including the 2009 Personal Information Protection Act.[117] The Personal Information Protection Act protects the personal information of Alaska consumers,[118] requiring that corporations notify consumers if they suffer a security breach that endangers consumers' personal information.[119] While the law does not mention biometric information, it defines "personal information" as the consumer's name coupled with another identifier, such as a Social Security number or driver's license number.[120] It also restricts the ways entities can use consumers' Social Security numbers.[121] It prohibits anyone from requesting, collecting, selling, or disclosing Social Security numbers, or making Social Security numbers public.[122]

Despite these protections, the Personal Information Protection Act still leaves Alaska consumers vulnerable to the collection of their most personal information: biometric information. While you can change your Social Security or driver's license numbers, your biometrics, specifically your faceprint, are inherent, unique, and constantly visible.[123] Further regulation is necessary to close the gaps that are allowing facial recognition technologies to spread in Alaska.

E. Anchorage Municipal Prohibition

While Alaska's privacy amendment paves the way for a judicial

116. See *id.* at 127 ("As already stated, Alaska's right to privacy generally protects two types of interests. One is an individual's interest in personal autonomy and independence in decision making. The other is an individual's interest in protecting 'sensitive personal information . . . which if, disclosed . . . could cause embarrassment[,] anxiety, humiliation, harassment, or economic or physical reprisals.'").
117. ALASKA STAT. § 45.48.010 (2009).
118. *Id.*
119. *Id.* § 45.48.030 (2009).
120. *Id.* § 45.48.090 (2009).
121. *Id.* § 45.48.420 (2009).
122. *Id.*
123. *See Biometric Information Privacy Act (BIPA)*, ACLU OF ILL. (2023), https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (last visited Feb. 3, 2024).

challenge to the use of facial recognition technologies by public actors, a statutory solution is an essential complement to this approach. Alaska has already made strides in regulating privacy at the municipal level. In April 2023, the Anchorage Assembly approved a municipal ordinance "to protect the right to privacy by codifying certain restrictions on the use of Facial Recognition Technologies by any municipal department or agency in a manner that's improper, surreptitious, or oversteps an individual's privacy rights."[124]

This ordinance establishes several safeguards on municipal use of technologically enhanced surveillance practices.[125] First, it restricts the municipality's use of "unmanned aircraft systems" (drones).[126] The ordinance also requires annual reporting on the use of drones by each department or agency.[127] These reports must be released to the assembly annually and posted on the municipal website for public viewing.[128]

Next, the ordinance severely restricts the use of facial recognition technologies.[129] It bans any use of real-time facial recognition surveillance[130] and further prohibits municipal staff from "obtain[ing], request[ing], access[ing], or us[ing]" any facial recognition technology or information obtained through its use.[131] Notably, it bans the use of any

124. Anchorage, Alaska, Ordinance No. 2023-35-(S-1) (Apr. 18, 2023) (amending the Anchorage Municipal Code Chapter 3, Section102).

125. *Id.*

126. *Id.*

127. *Id.* ("[F]or each municipal department and agency that used a UAS in the preceding calendar year: [report] (a) The number of instances in which a UAS was used; (b) A general description of the type and purpose of each use that sufficiently explains how the use was not prohibited by this chapter, and, if applicable, whether the use was pursuant to a search warrant, a court order, or a judicially recognized exception to the warrant requirement, and the final disposition of evidence resulting from each instance; and (c) Any new policy, or change in department or agency policy, related to the use of UAS or Facial Recognition Technology . . . . The annual report from the Anchorage Police Department shall also include: (a) The number of arrests made where UAS was utilized in a related incident response or investigation, regardless of whether the information gathered from the UAS was used to establish probable cause.").

128. *Id.* ("No later than June 1 of each year, the mayor or a designee shall transmit to the assembly and cause to be publicly posted on the municipal website a report . . . .").

129. *Id.*

130. *Id.*

131. *Id.* (noting that, however, "[m]unicipal staff's inadvertent or unintentional receipt, access of, or use of any information obtained from Facial Recognition Technology shall not be a violation of this section, provided that: (1) [m]unicipal staff did not request or solicit the receipt, access of, or use of such information: and (2) [m]unicipal staff logs such receipt, access, or use in its Annual Surveillance Report . . . . [S]uch report shall not include any personally identifiable information or other information the release of which is prohibited by law").

information obtained through facial recognition technology, even lawfully, in establishing probable cause to obtain a warrant.[132]

But the ordinance carves out several exceptions.[133] Some of these exceptions cover inadvertent use of facial recognition technologies.[134] For example, municipal employees are permitted to use single user devices with facial recognition capabilities, such as an iPhone.[135] Municipal employees may also use social media platforms that utilize facial recognition technology.[136] The other category of exceptions covers instances where Anchorage municipal officials or agencies might need to cooperate with other groups that use facial recognition.[137] For example, an exception is made for "[c]omplying with the National Child Search Assistance Act," or "other federal statutes requiring cooperation in the search for missing or exploited children."[138] Further, the ordinance states that "municipal law enforcement may intentionally work with third party agencies using Facial Recognition Technology to identify: human remains or suspected missing persons; suspected victims of human trafficking; or suspected victims of child abuse or exploitation."[139]

The ordinance also provides an avenue for municipal officers or

132. *Id.* ("Any evidence or information obtained through facial recognition technology, regardless of whether it was obtained lawfully, shall not be included in an affidavit to establish probable cause for purposes of issuance of a search warrant or an arrest warrant.")

133. *Id.*

134. *Id.* ("It shall not be a violation of this chapter for the municipality to acquire, obtain, or retain facial recognition technology when all the following conditions exist: (1) [t]he facial recognition technology is an integrated, off the shelf capability, bundled with software or stored on a product or device; (2) [o]ther functions of the software, product, or device are necessary or beneficial to the performance of municipal functions; (3) [t]he software, product, or device is not acquired for the purpose of performing facial recognition; (4) [t]he facial recognition technology cannot be deleted from the software, product, or device; (5) [t]he municipality does not use the facial recognition technology; and (6) [t]he municipal department, agency or official seeking to acquire the software, product, or device discloses the integrated, off the shelf facial recognition technology that cannot be deleted to the Assembly when seeking to acquire the software, product, or device.")

135. *Id.* (describing an exception to the facial recognition ban for "[a]cquiring, obtaining, retaining, or accessing facial recognition technology on an electronic device intended for a single user, such as a mobile communication device, cellular phone or tablet, when the facial recognition technology is used solely for the purpose of the user . . .").

136. *Id.* (outlining an exception for "[a]cquiring, obtaining, retaining, or accessing social media or communications software or applications intended for communication with the general public that include facial recognition technology, as long as the municipality does not intentionally use the facial recognition technology . . .").

137. *Id.*

138. *Id.*

139. *Id.*

agencies to request an exception that is not specifically enumerated.[140] In order to be granted an exception, the requesting department must detail their need for the exception, coupled with a plan "for monitoring the technology or information to ensure that its use remains within the approved parameters."[141] Then, the assembly must hold a public hearing to determine whether the exception is "consistent with the stated goals of preventing discrimination and promoting privacy, transparency, and the public trust."[142] Whether permanent or temporary, departments that have been granted an exception must submit reports detailing their expected use of the technologies.[143]

The ordinance also contains stringent reporting standards.[144] It requires that the municipality prepare an "Annual Surveillance Report" and post it publicly each year.[145] This report must contain information on each time an Unmanned Aircraft System or Facial Recognition Technology was used.[146] The ordinance also requires the municipality to report "every unauthorized receipt, access, or use of Facial Recognition Technology or information derived from Facial Recognition Technology."[147]

Finally, the ordinance provides multiple avenues to enforce its ban on drones and facial recognition technology.[148] Municipal employees who violate the ordinance may be suspended or terminated.[149] The ordinance also authorizes a private cause of action, so harmed citizens may bring suit against the municipality or third party contractors.[150] If a citizen sues under this cause of action and prevails, they are entitled to the greater of $1,000 per violation, or $10,000.[151] Prevailing plaintiffs are also entitled to

140. *Id.* ("Recognizing that changes in technology and circumstances may require additional exceptions to the requirements of this section, the assembly may approve such additional exceptions by resolution . . . .").
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.* ("The log shall denote how the unauthorized access occurred, what corrective steps have been taken, and the final disposition of any evidence or information improperly received.").
148. *Id.*
149. *Id.*
150. *Id.*
151. *Id.* ("Any person who has instituted proceedings under the previous paragraph and is found to have been subjected to face surveillance in violation of this article, or about whom data or information is found to have been obtained, retained, stored, possessed, accessed, used, or collected in violation of this article, shall be entitled to recover actual damages . . . .").

reasonable costs and attorney's fees.[152]

The sponsoring Assembly Members cited three main reasons for proposing this ordinance.[153] First, they pointed out flaws in the technology.[154] One sponsoring assembly member, Joey Sweet, said "[r]esearch shows that the technology in use across the country disproportionately misidentifies people of color most frequently of all demographics."[155] Second, they noted that facial recognition technologies impede Alaskans' privacy rights.[156] Third, assembly members expressed concerns that the use or misuse of the technology could expose the municipality to civil liability. Sweet said, "[t]his prohibition minimizes risk exposure to the Municipality while establishing a path to request exemptions."[157]

While this ordinance is ground-breaking in its regulation of municipal activity, it still leaves room for individuals and corporations to misuse facial recognition technologies. Sweet acknowledged this gap but felt that advancing an outright ban was beyond his capabilities as a temporary assembly member.[158] However, he continues to advocate for a total, statewide ban.[159] He hopes that Alaska "can kind of step up to the plate."[160] Indeed, a statewide ban would close the gap in privacy regulations that have allowed for the unchecked use of these technologies by both public and private actors.

IV. ILLINOIS AS A POTENTIAL MODEL FOR STATEWIDE

152. *Id.*

153. Press Release, Anchorage Assembly, Assembly Approves Ban on Facial Recognition Technology (Apr. 18, 2023), https://www.muni.org/Departments/Assembly/PressReleases/Pages/Assembly-Approves-Ban-on-Facial-Recognition-Technology.aspx.

154. *Id.*

155. *Id.*

156. *See id.* ("The second is how the technology infringes on residents' right to privacy, which is particularly steadfast in our state.").

157. *Id.*

158. James Brooks, *Facial Recognition Remains Unregulated in Alaska, Even as It Grows in Use*, ALASKA PUB. MEDIA (July 19, 2023), https://alaskapublic.org/2023/07/19/facial-recognition-remains-unregulated-in-alaska-even-as-it-grows-in-use/.

159. *Id.* ("[T]here's nothing stopping Walmart, or Fred Meyer, or anyone, from investing in that kind of security, and then saying, 'Oh, here's this poor person we saw steal some bread last week, let's scan their face into some shadowy database, and then the next time we see them, we can just give them the boot immediately.' I don't think that's an acceptable situation, to say nothing of the fact that it can go wrong and misidentify people.").

160. *Id.*

INTERVENTION

Illinois' Biometric Information Privacy Act (BIPA)[161] offers a possible model for a statewide reform in Alaska. It is widely regarded as one of the toughest biometric privacy laws in the country.[162] BIPA was passed unanimously in 2008 in response to growing concerns about private corporations increasingly using biometric identifiers[163] for transactions and security purposes.[164] The Illinois legislature noted that citizens were hesitant to embrace these developments: "[a]n overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information."[165]

BIPA mandates that private entities[166] that collect biometric identifiers publicize their compliance with certain guidelines.[167] They must establish a schedule for retention and a plan to permanently destroy the information once its purpose has been served.[168] In addition to these guidelines, private entities may not collect biometric identifiers without informing individuals in writing that their information is being collected.[169] Entities must also inform individuals of how long their information is being used and what it is being used for.[170] After these disclosures, entities must receive a written release from individuals, consenting to the use of their biometric information.[171] BIPA also prohibits the sale or trade of biometric information.[172] And finally, it

161. Biometric Information Privacy Act, 740 Ill. Comp. Stat. Ann. 14/15 (West 2023).

162. ACLU of Illinois, *What is BIPA?*, ACLU OF ILL. (2023), https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.

163. *See* 740 Ill. Comp. Stat. Ann. 14/10 (defining biometric identifier as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry").

164. *Id.* 14/5 ("Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.").

165. *Id.*

166. *See id.* (defining private entity as "any individual, partnership, corporation, limited liability company, association, or other group, however organized").

167. *Id.*

168. *See id.* ("A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.").

169. *Id.*

170. *Id.*

171. *Id.*

172. *Id.*

establishes a private right of action for individuals who have had their biometric information used without their consent.[173]

In 2020, the ACLU and several other plaintiffs sued Clearview AI in Illinois, alleging that it violated BIPA.[174] Plaintiffs expressed concerns about the use of faceprints generally,[175] and about the unprecedented scale of Clearview's database, specifically.[176] They further noted that other technology companies have long had the capability to create a database like Clearview's, but refused due to ethical concerns.[177] Given the massive scale of Clearview's database, plaintiffs cited lack of security controls as a major concern.[178] In support of this proposition, plaintiffs noted the leak of Clearview's secret client list, as well as a server error exposing the company's internal files to the internet at large.[179]

Plaintiffs specifically alleged that Clearview AI violated Section 1.5(b) of BIPA by "captur[ing], us[ing], and stor[ing]" the biometric identifiers of countless Illinois residents[180] without informing them or obtaining written consent.[181] Plaintiffs further alleged that Clearview failed to "provide a retention schedule or guidelines for permanently destroying individuals' biometric identifiers as required by the BIPA."[182] Clearview moved to dismiss this suit, citing "a variety of constitutional, common law and statutory arguments."[183] Most notably, Clearview

173. *Id.*

174. ACLU v. Clearview AI (*Clearview II*), No. 2020 CH 04353, 2022 U.S. LEXIS 2887 (Ill. Cir. Ct. May 11, 2022).

175. *See* Complaint at 10, *Clearview II* (discussing the risks of a malicious third party breach of biometric data as "especially harmful because unlike numerical identifiers (e.g. Social Security Numbers), which can be replaced or re-assigned, biometrics are biologically unique to each person and therefore, once exposed, an individual has no recourse to prevent falling prey to misconduct like identity theft and unauthorized tracking").

176. *See id.* at 19 ("Clearview has set out to do what many companies have intentionally avoided out of ethical concerns: create a mass database of billions of faceprints of people, including millions of Illinoisans, entirely unbeknownst to those people, and offer paid access to that database to private and governmental actors worldwide.").

177. *Id.*

178. *Id.* at 20 ("[I]n an age where companies spend huge amounts of money on dedicated information security personnel and infrastructure in order to secure sensitive information, it is likely that Clearview lacks even remotely sufficient security controls.").

179. *Id.*

180. *See id.* at 23 ("The extraordinary breadth and volume of online photos used by Clearview to capture faceprints for its database means that it is a near certainty that anyone whose photos are posted to publicly accessible portions of the internet will have been subjected to surreptitious and nonconsensual faceprinting by Clearview.").

181. *Id.* at 31.

182. *Id*. at 32.

183. ACLU v. Clearview AI (*Clearview I*), No. 20 CH 4353, U.S. LEXIS 292 (Ill.

argued that BIPA should not apply to "Clearview's collection of biometric data from publicly-available photos."[184] The court denied this motion to dismiss on the grounds that it had proper jurisdiction and the complaint stated "a cause of action for which relief may be granted."[185] The parties reached a settlement before the case went to trial.[186]

This groundbreaking settlement, largely regarded as a massive win for consumer privacy rights,[187] made a nationwide impact. First, it enjoined Clearview from offering access to its database to *any* private entity nationwide, except in compliance with BIPA.[188] Second, it enjoined Clearview from offering access to its database to any "Illinois state, county, local, or other government agencies and contractors working for those agencies in Illinois, including state and local police departments and other state and local law enforcement agencies" for five years.[189] It also forced Clearview to delete facial scans developed before the settlement.[190] Additionally, Clearview agreed to maintain and promote a publicly-available site allowing Illinois residents to opt out of their database.[191] Clearview further agreed to attempt to screen Illinois residents from entering their databases for five years.[192]

Given the success and impact of BIPA in Illinois, the Alaska legislature should strive to pass similar legislation. It should prevent private actors from maintaining and utilizing vast databases of Alaskans' biometric information. This approach, coupled with judicial enforcement of the constitutional privacy right as outlined in Part III of this Note, would ensure that Alaskans are protected from the misuse of their biometric information from both public and private actors.

Cir. Ct. Aug. 27, 2021) at *5.

184. *Id.*; *see also id.* at *12 (reasoning that BIPA does apply to Clearview's use of photos to create face scans. BIPA defines "a scan of face geometry" as a protected "biometric identifier." The court reasoned that "[t]he fact that the scan was made from a photo and not from a live person does not change that fact.").

185. *Id.* at *25–26.

186. *See generally Clearview II.*

187. *See In Big Win, Settlement Ensures Clearview AI Complies with Groundbreaking Illinois Biometric Privacy Law*, ACLU (May 9, 2022) https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois ("By requiring Clearview to comply with Illinois' pathbreaking biometric privacy law not just in the state, but across the country, this settlement demonstrates that strong privacy laws can provide real protections against abuse.").

188. Settlement Agreement at 1–2, *Clearview II*.

189. *Id.*

190. *Id.* at 3.

191. *Id.* at 4.

192. *Id.*

V. CONCLUSION

The growing ubiquity of facial recognition AI is a pressing issue.[193] The growth of this technology threatens to wholly erode privacy forever. But it is not too late to stop its spread. While federal regulation is lagging, states can enact meaningful legislation for their citizens. Alaska is perfectly situated to do this for the reasons outlined in this Note. In the future, as facial recognition capabilities grow and its usage spreads, Alaska can serve as a haven of privacy for its citizens and visitors.

193. *See* Rebecca Heilweil, *From Macy's to Albertsons, Facial Recognition is Already Everywhere,* VOX (July 19, 2021) https://www.vox.com/2021/7/15/22577876/macys-fight-for-the-future-facial-recognition-artificial-intelligence-stores. ("A lot of people would probably be surprised to know how many retailers that they shop in on a regular basis are using this technology in a variety of ways to protect their profits and maximize their profits as well.").