University of Cincinnati Law Review

Volume 89 | Issue 1 Article 2

October 2020

Big Brother is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century

Samuel D. Hodge Jr.
Temple University

BIG BROTHER IS WATCHING: LAW ENFORCEMENT'S USE OF DIGITAL TECHNOLOGY IN THE TWENTY-FIRST CENTURY

Samuel D. Hodge, Jr.[1]

There was of course no way of knowing whether you were being watched at any given moment.
- George Orwell, 1984

"Big brother is watching" is a phrase coined by George Orwell in his novel *1984*. This saying describes the government's surveillance of its citizens with electronic listening devices and cameras in a jurisdiction where Big Brother is the head of a totalitarian administration.[2] The phrase depicts an attitude in which no one is beyond the reach of a prying government that uses digital cameras with facial recognition software and may result in the incarceration of anyone who opposes the regime.[3] Penned by Orwell in 1947, the fictionalization was meant to provide a forum to discuss "surveillance, police states and authoritarianism."[4] More than seventy years later, the book has proven to be prophetic. The same technological breakthroughs that have changed our lives have also produced detailed records of our daily lives.[5]

To protect society against the dangers presented by terrorism, the government has demonstrated a profound desire to secure as much data as possible and to utilize that digital information for a variety of purposes.[6] This article will examine some of the innovations used by law enforcement for observation and identification purposes, such as video surveillance, drones, automated license plate readers, and facial recognition software. Though each tool is different, the legal issues

---

1. Samuel D. Hodge, Jr. is an award winning professor at Temple University where he teaches law, anatomy and forensics. He is also a member of the Dispute Resolution Institute where he serves as a mediator and neutral arbitrator. He is one of the most published scholars in medical/legal matters and has authored more than 180 articles in medical and legal journals and has written ten texts including *The Forensic Autopsy*. He also enjoys an AV preeminent rating and has been named a top lawyer in Pennsylvania on multiple occasions. The author wishes to thank Nallely Barbosa, a recent graduate of the Temple University Beasley School of Law and a teaching assistant for Professor Hodge, for her invaluable research and editorial assistance.

2. *Big Brother is Watching You,* LITERARY DEVICES, https://literarydevices.net/big-brother-is-watching-you/ Z (last visited Nov. 28, 2019).

3. *Id.*

4. Matthew Feeney, *Seventy Years Later, It's Still '1984'*, CATO INSTITUTE (JUNE 5, 2019), https://www.cato.org/publications/commentary/seventy-years-later-its-still-1984?gclid=Cj0KCQiA2vjuBRCqARIsAJL5a-KKoOpz0zDd5WcM2avykIIvE_pz4qeeI05VB_hPCBIgAaF7thCii1waAtgaEALw_wcB.

5. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934 (2013).

6. *Id.*

involving the various forms of digital technology are relatively similar.

I. VIDEO SURVEILLANCE

Members of society are observed through surveillance equipment in many settings such as the streets, banks, casinos, stores, and shopping malls.[7] Routine monitoring takes place as we drive a vehicle or walk along a sidewalk, thereby offering a comprehensive picture of our private lives.[8] Roughly three-quarters of small businesses record those who enter their premises[9] and closed-circuit television (CCTV) systems even allow law enforcement officials to detect, prevent, and investigate assaults and to discover crimes against property.[10]

The first use of cameras for surveillance purposes occurred in England in 1986 where the equipment was installed in a one-square-mile area in the town of King's Lynn.[11] Today, England is the worldwide leading user of closed-circuit monitoring systems with one-half million cameras in its network. Several years later, a few cities in the United States, such as Philadelphia, Chicago, and New York, followed England's lead and started installing surveillance cameras in public areas.[12] For instance, Chicago maintains about 3,700 surveillance cameras and has access to more than 32,000 others which can be monitored at police districts, public safety headquarters, and other law enforcement locations.[13] The City also utilizes cameras on police and fire boats, helicopters, SUVs, trailers, and command vehicles.[14] Nationally, the use of surveillance equipment is even more dramatic. Approximately 30 million cameras are employed in the United States filming 4 billion hours of footage a week. Needless to say, Big Brother is watching almost everywhere and most of the time.[15]

7. JERRY RATCIFFE, VIDEO SURVEILLANCE OF PUBLIC PLACES (Center for Problem-Oriented Policing, Response Guide No. 4, 2006), *available at* https://popcenter.asu.edu/content/video-surveillance-public-places-0.

8. Amanda Li, *Top 8 Pros and Cons of Surveillance Cameras in Public Places*, REOLINK (Aug. 28, 2019), https://reolink.com/pros-cons-of-surveillance-cameras-in-public-places/.

9. Ratciffe, *supra* note 7.

10. Qasim Mahmood Rajpoot & Christian Damsgaard Jensen, *Video Surveillance: Privacy Issues and Legal Compliance*, DTU (2015), https://backend.orbit.dtu.dk/ws/portalfiles/portal/110934780/Video_Surveillance_Privacy_issues_and_legal_compliance.pdf.

11. Cristen Conger, *Do Police Cameras Reduce Crime*, HOW STUFF WORKS, https://electronics.howstuffworks.com/police-camera-crime.htm (last visited Dec. 1, 2019).

12. *Id.*

13. Scott Goldfine, *32K Surveillance Cameras Aim to Keep Chicago Safe*, CAMPUS SAFETY (Oct. 31, 2018), https://www.campussafetymagazine.com/technology/surveillance-cameras-keeping-chicago-safe/.

14. *Id.*

15. James Vlahos, *Surveillance Society: New High-Tech Cameras Are Watching You*, POPULAR MECHANICS (Oct. 1, 2009), https://www.popularmechanics.com/military/a2398/4236865/.

This surveillance will only increase as the price of equipment falls, making it feasible to assemble a heretofore unimaginable quantity and quality of data.[16] The bottom line is that society is moving towards an environment in which a person's every move and transaction is recorded by a computer or system.[17]

These recorded observations are not limited to police use. Consumer spending for home surveillance equipment, such as doorbell cameras, will grow into a $9.7 billion industry by 2023.[18] This development has resulted in private outdoor cameras on homes becoming an emergent law enforcement tool.[19] For example, 400 police departments have partnered with one doorbell camera company to gain access to its footage to assist in solving home thefts, vehicle break-ins, and other crimes.[20] The widespread use of such equipment has also made it standard police practice to search for video cameras in the area of a reported crime, making them important tools for fighting criminality and gradually supplanting neighborhood watch groups and its legion of invisible street guardians.[21]

A. Video Surveillance Equipment

Video surveillance equipment consists of a camera that is usually hooked up to a recording device or IP network. This video data is then arranged into a searchable database through biometric software, thereby making the viewing process more efficient for law enforcement purposes.[22] The cameras can also be armed with motion-detecting sensors, which vastly diminish the amount of data and further enhance the efficiency of the viewing task.[23] The equipment is now so sophisticated that cameras permit users to take advantage of "satellite-based optics" that allow the observer to see in the dark, visualize words on a page hundreds

16. *Id.*

17. *Id.*

18. T.J. McCue, *Home Security Cameras Market to Surpass $9.7 Billion By 2023*, FORBES (Jan. 31, 2019), https://www.forbes.com/sites/tjmccue/2019/01/31/home-security-cameras-market-to-surpass-9-7-billion-by-2023/#3f3bea523c2b.

19. *Watchful Help or Harm?: Police Access Home Surveillance Cameras To Solve Crimes*, PITTSBURGH POST-GAZETTE (Sep. 30, 2019), https://www.post-gazette.com/opinion/editorials/2019/09/30/Home-surveillance-cameras-Ring-Amazon-police/stories/201909280013.

20. *Id.*

21. Faith Karimi, *Home Surveillance Cameras Are The New Neighborhood Watch*, CNN (Aug. 31, 2018), https://www.cnn.com/2018/08/30/us/home-surveillance-cameras-neighborhood-watch/index.html.

22. *Jack Giordano*, VIDEO EVIDENCE: LEGAL STANDARDS & PRACTICAL CONSIDERATIONS *(2017), available at 2017 WL 6944772.*

23. *Id.*

of feet away, and look into buildings.[24]

B. Benefits of Surveillance Cameras

Surveillance cameras in public places have the benefit of identifying the perpetrator of a crime.[25] The Boston Marathon bombing provides an example. The government was able to release images of the two suspects from a surveillance camera installed on the outside wall of a department store just three days after the attack.[26] The technology can also provide a feeling of enhanced safety. The cameras can visualize a large area or focus on a specific location known for criminal activity. The technology may even act as a deterrent in stopping an offense if the criminal knows that a camera is filming the location.[27] The footage can also protect the innocent by preventing the police from identifying and arresting the wrong individual.

In a legal setting, the footage provides a very strong piece of evidence since it is nearly impossible to maintain that a suspect captured on an image is not the perpetrator of the crime.[28] Surveillance cameras can also prevent fraud and made-up stories. For example, a video recording of an alleged crime or motor vehicle accident can easily disprove a fraudulent claim, thereby freeing up valuable investigative time.[29]

C. Criticisms of Surveillance Cameras

A variety of challenges have attacked the use of video surveillance systems, including concerns about the databases that store the video footage, the failure to enact standards regulating the retention and use of the data collected, and the risk for geolocation tracking without necessary oversight.[30] Unfortunately, there is a paucity of laws on the use of surveillance cameras in public places, and only a small number of jurisdictions have enacted legislation to regulate these activities. New York's statute, for example, provides that law enforcement officials may only use this technology as part of an investigation of suspected criminals after obtaining a warrant from the court.[31]

---

24. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and The Right to Anonymity*, 72 MISS. L.J. 213, 220 (2002).

25. Li, *supra* note 8.

26. *Id.*

27. *Security Cameras in Public Places: A Good or Bad Thing?*, TITAN ALARM (Oct. 3, 2017), https://titanalarm.com/security-cameras-in-public-places-a-good-or-bad-thing/.

28. *Id.*

29. *Id.*

30. Kimberly Winbush, Annotation, *Use of License Plate Readers*, 32 A.L.R.7th Art. 8, § 2 (2017).

31. Li, *supra* note 8.

Surprisingly, the widespread employment of video cameras has not reduced crime and its use is not embraced by all people.[32] For instance, one study revealed that closed-circuit camera systems did not generate "enough bang for the buck."[33] While Federal and state governments have spent millions to install and maintain these systems, the study demonstrated that the equipment was underemployed and not properly assimilated into police strategies.[34]

Another major criticism of video surveillance is its potential for abuse by law enforcement. A story in the *Detroit Free Press* supports this concern, revealing that law enforcement officials in Michigan used the equipment to assist both themselves and their friends stalk females, threaten motorists after traffic incidents, and track former spouses or partners.[35] The technology also raises privacy concerns, since advancements in surveillance equipment often outpace changes in the law regulating new developments.[36]

While Society is indeed exposed to serious security challenges, placing cameras in public areas is not universally accepted as a method of safeguarding the public. Cameras in public areas will inevitably film innocent individuals who have no intention of committing a crime and some feel that this constitutes an invasion of privacy.[37] Some would rather preserve their privacy than feel that "Big Brother" is watching their every move.[38]

The Fourth Amendment is designed to protect against unreasonable search and seizure, and additional safeguards are derived from legislation and case law.[39] However, it may take years before the courts or legislatures address the thorny issues raised by privacy concerns, as new developments in video technology continue to develop on a rapid and regular basis.[40] Questions are also expressed about how the footage is being stored and protected, who has access to the images, under what circumstances can it be retrieved, and whether it can be coupled with other

32. *What's Wrong With Public Video Surveillance?*, ACLU, https://www.aclu.org/other/whats-wrong-public-video-surveillance (last visited Nov. 28, 2019).

33. Conger, *supra* note 11.

34. *Id.*

35. *Id.* In 1998, a police lieutenant From D.C. Was Criminally Charged For "Extorting Money from Customers of a Gay Bar." The Evidence Revealed That He Wrote Down the License Plate Numbers of Those Visiting the Bar and Bribed Them into Paying Him Money by Threatening "To Expose Their Lifestyle." Lauren Fash, Comment, *Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy*, 78 MD. L. REV. ONLINE 63 (2019).

36. Allyssa Nielson, *Video Surveillance Threatens Privacy, Experts Say*, DAILY UNIVERSE (June 28, 2017), https://universe.byu.edu/2017/06/28/video-surveillance-threatens-privacy/.

37. *Security Cameras in Public Places: A Good or Bad Thing?*, *supra* note 27.

38. *Id.*

39. Nielson, *supra* note 36.

40. *Id.*

materials to create a profile of a person.[41]

D. Video Surveillance and the Fourth Amendment

Video surveillance is one of the most intrusive types of searches performed by the government,[42] and the courts will consider the expectations of society when measuring its constitutionality.[43] One court indeed observed that "[t]his type of surveillance provokes an immediate negative visceral reaction: indiscriminate video surveillance raises the specter of the Orwellian state."[44]

Generally speaking, the courts have not deemed video surveillance of a public area to be a search since the person being observed fails to have a reasonable expectation of privacy.[45] *State v. Augafa* provides an example in which the court found that video surveillance of a public area is not an invasion of privacy, nor is it a violation of the Fourth Amendment against unreasonable search and seizure.[46] In *Augafa*, the defendant was filmed selling drugs on a public sidewalk. Since this illegal activity was observed in "open view," no reasonable expectation of privacy was applicable, and the surveillance was not within the ambit of the Constitution.[47] The Intermediate Court of Appeals of Hawaii noted that a privacy test requires the court to decide "whether a person's expectation of privacy under any particular set of circumstances may be deemed reasonable."[48] A violation of the Fourth Amendment only occurs when it can be shown that an actual, subjective expectation of privacy is present, and that the expectation is one that society acknowledges as being objectively reasonable.[49]

In another case, a federal district court found that the installation of two video cameras by the police—one on a pole outside an apartment building and one in a hallway—is not a search under the Fourth Amendment.[50] As noted: "The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[51] This guarantee is linked to the notion of a common law trespass and considers whether the police secured

41. *Id.*
42. United States v. Cuevas–Sanchez, 821 F.2d 248, 250–51 (5th Cir. 1987).
43. *Id.* at 251.
44. *Id.*
45. Florida v. Riley, 488 U.S. 445, 449 (1989).
46. State v. Augafa, 992 P.2d 723, 725 (Haw. Ct. App.1999).
47. *Id.* at 734.
48. *Id.* at 733.
49. *Id.*
50. United States v. Kelly, 385 F. Supp. 721, 727 (E.D. Wis. 2019).
51. *Id.* at 726.

information by physically intruding upon a constitutionally protected area.[52] This concept was later transformed into one that protects people and their reasonable expectation of privacy.[53] In this regard, the court held that a tenant does not enjoy a reasonable expectation of privacy in the common areas of an apartment building.[54]

Several courts have considered whether long-term video surveillance of a house from a pole camera constitutes a "search" under the Fourth Amendment.[55] These courts have generally found that such a practice is constitutional because "a pole camera only captures events that a police officer or utility worker situated on the pole could see."[56] The decisions have found that extended police observation from a pole camera is deemed irrelevant to their "search" analysis.[57] For example, in *U.S v. Houston*, the Sixth Circuit Court of Appeals ruled that video surveillance performed over ten weeks from a utility pole 200 yards away from a property did not violate the defendant's reasonable expectation of privacy because the camera recorded the same view that a passerby would have from the street.[58] Since government agents could have been positioned 24-hours a day to watch the property, the fact that a camera was used to conduct the surveillance fails to make it unconstitutional.[59]

A contrary result was reached in *People v. Tafoya*, where a Colorado appellate court found it unconstitutional for the police to have placed a video camera on a pole near the defendant's house to surveil it over a lengthy period.[60] This camera continually observed the property, including an area behind the owner's fence, for more than three months.[61] Based on these prolonged observations, the police obtained a warrant to search the defendant's property where they found a cache of drugs.[62]

The court acknowledged that it would have been permissible for an officer to climb to the top of the utility pole and look over the defendant's fence with binoculars or with a telescopic camera. However, it was improper to install a video camera that allowed the police to perform continuous surveillance of the property, including the space

52. *Id.*

53. *Id.*

54. *Id.* at 727.

55. *People v. Tafoya*, No. 17CA1243, 2019 Colo. App. LEXIS 1799, at *13 (Colo. App. Nov. 27, 2019).

56. *Id.* at *12-13.

57. *Id.* at *13-14.

58. United States v. Houston, 813 F.3d 282 (6thCir.2016).

59. *Id.* at 288.

60. *Tafoya*, 2019 Colo App. LEXIS 1799, at *25-26.

61. *Id.* at *1.

62. *Id.* at *1-2.

behind the owner's privacy fence, from the police station for more than three months.[63] The court opined that "unfettered use of surveillance technology could fundamentally alter the relationship between our government and its citizens."[64] This type of conduct, the court determined, is inconsistent with an open and free society.[65]

A more difficult Fourth Amendment determination occurs when video surveillance is conducted in a private setting. The following two cases illustrate the problem. In *Hernadez v. Hillsides, Inc*., an employer was found not to have committed tortious invasion of privacy when it set up a hidden camera in the office of two employees to ascertain who was viewing pornographic websites at night in a residential facility for abused and neglected children.[66] The California Supreme Court determined that while a jury could conclude that the employer intruded upon the workers' reasonable privacy expectations, the intrusion was not highly offensive or egregious enough to violate prevailing social norms. Activation of the video system was restricted to the night when the plaintiffs were working.[67]

A contrary result was reached in *Carter v. County of Los Angeles* where a hidden camera was placed in a fake smoke detector.[68] A report had been made that one of the Department of Public Works' employees had engaged in a sexual act with a visitor in the dispatch room.[69] A hidden camera installed in that area captured inappropriate conduct by several employees with visitors.[70] The plaintiffs eventually discovered the camera and claimed that their Fourth Amendment rights against unreasonable search and seizure were violated by the secret recordings.[71] A federal district court agreed and noted that the employees' belief that "they were free from video surveillance was reasonable."[72] They worked in a secure, private, and often solitary room that was used for work and off-duty activities like eating and napping.[73] While employers have many tools available to investigate allegations of worker wrongdoing, covert video surveillance is not one of them.[74]

63. *Id.* at *25-26.
64. *Id.* at *15.
65. *Id.* at *16.
66. Hernadez v. Hillsides, Inc., 211 P.3d 1063, 1066 (Cal. 2009).
67. *Id.* at 1082.
68. Carter v. County of L.A., 770 F. Supp. 2d 1042, 1046 (C. D. Cal. 2011).
69. *Id.* at 1045-46.
70. *Id.* at 1046.
71. *Id.* at 1047.
72. *Id.* at 1049.
73. *Id.* at 1047.
74. *Id.* at 1050.

II. AUTOMATIC LICENSE PLATE READERS

The automated license plate reader ("ALPR") is the most employed law enforcement surveillance tool.[75] The system consists of high-speed cameras that photograph each license plate that passes by the devices[76] and operates on infrared and visual light spectrums so that the plates can be read at all times.[77] These readers can be placed anywhere from police vehicles to stationary objects like poles, traffic lights, and overpasses.[78] As noted by the Supreme Court of Ohio in *State v. Hawkins:*

> A license-plate reader is a computer-controlled camera system installed in some law-enforcement vehicles. The cameras, which are mounted to the trunk of the vehicle, capture images of the license plates of cars nearby. The system beeps to alert the officer that a plate has been captured, and an image of the plate is displayed on the computer's screen.[79]

ALPRs can image about 2,000 license plates per minute on vehicles going about 120 miles per hour.[80] Apps are even available that permit beat cops to scan license plates with their smartphones.[81] In turn, the images are transmitted and analyzed by a computer that identifies the owner of the vehicle, affixes a time and location stamp, and uploads the images to a central server.[82]

A. Police Use of ALPRs

ALPRs permit law enforcement to identify and record a vehicle's whereabouts in real-time and determine its prior locations.[83] Generally, the system will compare each license plate number against "hotlists" to sound an instant warning when a match or "hit" appears.[84] It can also

75. Dave Maass, *The Four Flavors of Automated License Plate Reader Technology*, ELECTRONIC FRONTIER FOUND. (Apr. 6, 2017), https://www.eff.org/deeplinks/2017/04/four-flavors-automated-license-plate-reader-technology.

76. *Id.*

77. Kelsey D. Atherton, *License Plate Readers Are Photographing You Everywhere*, POPULAR SCI. (June 27, 2013), https://www.popsci.com/technology/article/2013-06/license-plate-readers-automatically-create-big-data/.

78. *You Are Being Tracked*, ACLU 4 (July 2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.

79. State v. Hawkins, *158 Ohio St. 3d 94, 95, 2019-Ohio-4210, 140 N.E.3d 577.*

80. Justin Rohrlich, *In Just Two Years, 9,000 of These Cameras Were Installed to Spy on Your Car*, QUARTZ (Feb. 5, 2019), https://qz.com/1540488/in-just-two-years-9000-of-these-cameras-were-installed-to-spy-on-your-car/.

81. *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, *supra* note 78, at 4.

82. Maass, *supra* note 75.

83. *Id.*

84. *You Are Being Tracked*, *supra* note 78, at 2.

retrieve vast amounts of information from the National Crime Information Center on vehicles and license plates, which in turn can identify wanted persons, protection from abuse orders, missing persons, gangs, suspected terrorists, and immigration violators.[85] Other applications include the ability to verify witness descriptions of vehicles and identify cars that were near a specific site.[86] In turn, this data can be stored for weeks, months, or years.[87] Notably, most license plate numbers imaged by these systems do not match stolen vehicle lists and have no apparent link to any crimes, AMBER alerts, or warrants.[88] Studies estimate that the number of license plate scans linked to a crime is only around 0.2 percent.[89]

B. Legal Issues with ALPRs

The use of ALPRs creates legal issues because the data is stored on a computer that is often linked with regional sharing systems, thereby creating huge databases of driver location information. This information is frequently retained and shared with others with few restrictions on how it can be used.[90] Critics maintain that this technology presents major privacy and "other civil liberties threats."[91]

The Fourth Amendment and its interpretation by the courts controls how government officials can accumulate data obtained by ALPRs.[92] The litmus test for what constitutes an unlawful search was established by the Supreme Court in *Katz v. United States* where the Court stated "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[93]

The harm caused by one scan seems minuscule.[94] The rub is that the

85. Julia M. Brooks, *Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia*, 25 RICH. J.L. & TECH. 3, 2019, at P3.

86. Nat'l Ass'n of Criminal Defense Lawyers, Automated License Plate Readers (2016), *available at* https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-4-28_ALPR-Primer_Final.pdf.

87. *Id.*

88. Am. Civil Liberties Union Found. v. Superior Court, 400 P.3d 432, 435 (Cal. 2017).

89. Stephanie Foster, *Should the Use of Automated License Plate Readers Constitute A Search After Carpenter v. United States?*, 97 WASH. U. L. Rev. 221, 226-27 (2019).

90. Nat'l Ass'n of Criminal Defense Lawyers, *supra* note 86.

91. *Id.*

92. *Scott Bomboy, Police Photos of Your License Plates and the Fourth Amendment*, *YAHOO! NEWS* (July 19, 2013), https://www.yahoo.com/news/police-photos-license-plates-fourth-amendment-132009696.html?guccounter=1.

93. Katz v. United States, 389 U.S. 347, 351 (1967).

94. Michael Fisher, *Ohio Is Jonesing for Automatic License Plate Readers: Why This May Violate Your Fourth Amendment Rights and What the Ohio Legislature Should Do About It*, 64 CLEV. ST. L. REV. 329, 330 (2016).

use of cameras coupled with the widespread sharing of that information provides law enforcement with the ability to put together the separate puzzle pieces of where people have been into a single, high-resolution snapshot of their lives.[95] Studies of jurisdictions that utilize license plate recognition systems show that Fourth Amendment concerns are not out of line. One study revealed that for every one million license plates scanned in Maryland during one year, only forty-seven were theoretically related to "serious crimes."[96] Even though many states have the same low hit rate, law enforcement still collects and stores the data associated with these non-hit scans.[97] Therefore, license plate reader databases provide the opportunity for institutionalized abuse by allowing anyone who has access to the information to snoop into an individual's daily activities, habits, or present and past relationships.[98]

The American Civil Liberties Union and the Electronic Frontier Foundation maintain that these systems permit local, state, and federal agencies to follow the habits and locations of innocent individuals. They further assert that this data gathering constitutes an invasion of privacy and may be utilized to manipulate or exploit citizens if the surveillance data lands in the wrong hands.[99] ALPRs can also be utilized for discriminatory targeting. A law enforcement official who manually inserts information on a biased basis can check more license plates of a particular ethnic or racial group than he or she would without the technology.[100]

C. Court Decisions involving ALPRs

No reported decision exits on the validity of protracted location tracking using an ALPR. However, there are several federal and state court opinions that have determined that single-instance database checks of license plate numbers do not qualify as searches under the Fourth Amendment.[101] For example, the Ninth Circuit Court of Appeals ruled in *U.S. v. Diaz Castaneda* that a license plate check was not a search under the Fourth Amendment.[102] In this case, the police officer did not have any reason to conduct the license plate check. Nevertheless, the court noted that individuals do not enjoy a subjective expectation of privacy in their

95. *You Are Being Tracked*, *supra* note 78, at 2.

96. Fisher, *supra* note 94, at 331.

97. *Id.*

98. *You Are Being Tracked*, *supra* note 78, at 2.

99. *Things to Know About Automatic License Plate Readers*, PHYS.ORG (Sep. 15, 2015), https://phys.org/news/2015-09-automatic-plate-readers.html.

100. *You Are Being Tracked*, *supra* note 78, at 9.

101. Nat'l Ass'n of Criminal Defense Lawyers, *supra* note 86.

102. United States v. Diaz-Castaneda, 494 F.3d 1146, 1148 (9thCir. 2007).

license plates, and even if they did, the court concluded that society would not recognize this belief as reasonable.[103] License plates are visible on a car's exterior for anyone to see and are intended to provide information about a vehicle to the police and others.[104] It is not reasonable for a person to believe that his expectation of privacy has been breached when an officer sees what is visible and uses that information to check the status of the vehicle and its registered owner.[105]

A chink in the armor occurred in *Neal v. Fairfax County Police Department* when the Supreme Court of Virginia was asked to decide whether "the retention of information gathered and stored by a police department using an automated license plate reader" violated the state's Government Data Collection and Dissemination Practices Act.[106] This law is designed to "ensure safeguards for personal privacy by government agencies."[107] The plaintiff maintained that the police department's use of license plate readers violated the provision that information should not be gathered "unless the need for it has been clearly established in advance" of collecting that data.[108]

Initially, the court noted that a license plate number by itself is merely a mixture of letters and numbers "that [do] not describe, locate or index anything about anyone."[109] However, the images and data linked to each plate represent "personal information" as defined by the statute.[110] The pictures reveal not only the plate's number but the vehicle and the surrounding area. This data coupled with the GPS location, time, and date when the images were filmed "afford a basis for inferring personal characteristics, such as . . . things done by or to the individual who owns the vehicle, as well as a basis for inferring the presence of the individual who owns the vehicle in a certain location at a certain time."[111] Therefore, it was logical to infer that the image and related data is "personal information" as contemplated by "the legislature's intent to remedy the potential mischief posed by the extensive collection, maintenance, use and dissemination of personal information and the potential for misuse of such information."[112] The court remanded the case for further action

103. *Id.* at 1151.

104. *Id.*

105. *Id.*

106. Neal v. Fairfax Cnty. Police Dept, 812 S.E.2d 444, 445 (Va. 2018).

107. *Id.* at 339.

108. *Id.*

109. *Id.* at 346.

110. *Id.*

111. *Id.* at 346-47.

112. *Id.* at 347. *See also* United States. v. Ellison, 462 F.3d 557 (6th Cir. 2006); United States v. Matthews, 615 F.2d 1279, 1285 (10th Cir. 1980); United States v. Walraven, 892 F.2d 972 (10th Cir. 1989); Olabisiomotosho v. City of Hous., 185 F.3d 521 *(*5th Cir. 1999)*;* United States v.

consistent with its decision.[113]

One year later, the Circuit Court of Virginia reconsidered the issue.[114] While the ALPR record-keeping procedure does not per se "identify particulars" of a vehicle owner, it does permit law enforcement to link the information with the identity of an individual.[115] "In other words, access to the license plate number stored in the ALPR system 'permit[s] connection' to the identity of the vehicle's owner with a few clicks on the screen, all from the driver's seat of a police cruiser."[116] Therefore, the ALPR record-keeping process is a "passive use" as defined by the Data Act and a violation of the statute.[117] The court granted the plaintiff's request for an injunction barring law enforcement officials from photographing and storing random license plate data unless the plate was scanned according to "investigations of suspected criminal activity."[118] This decision has been hailed as a victory for data privacy rights advocates in their battle over the utilization of digital technologies by the police and other government officials.[119]

According to the National Conference of State Legislatures,[120] sixteen states have enacted statutes on ALPRs: Arkansas,[121] California,[122] Colorado,[123] Florida,[124] Georgia,[125] Maine,[126] Maryland,[127] Minnesota,[128]

Sparks, 37 Fed. Appx. 826, (8th Cir. 2002); and Hallstein v. City of Hermosa Beach, 87 Fed. Appx. 17 (9th Cir. 2003).

113. *Id.* at 350.

114. Neal v. Fairfax Cnty. Police Dep't, Case No. CL-2015-5902, Letter Opinion, Judge Robert J. Smith (Apr. 1, 2019), *available at* https://assets.documentcloud.org/documents/5805797/Opinion-190401-Alpr-Petition-Granted.pdf.

115. *Id.* at 5.

116. *Id.*

117. *Id.*

118. Cathy Wu, *Neal v. Fairfax County Police Department: Use of Automatic License Plate Reader Violates Data Privacy Law*, JOLTDIGEST (Apr. 22, 2019), https://jolt.law.harvard.edu/digest/neal-v-fairfax-county-police-department-use-of-automatic-license-plate-reader-violates-data-privacy-law.

119. *Id.*

120. *Automated License Plate Readers: State Statutes*, NCSL, http://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx (last visited Nov. 30, 2019).

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

128. *Id.*

Montana,[129] Nebraska,[130] New Hampshire,[131] North Carolina,[132] Oklahoma,[133] Tennessee,[134] Utah[135] and Vermont.[136] The specifics of these laws differ depending upon the jurisdiction and objective of the state.

Maine and New Hampshire have the most restrictive laws concerning the use of ALPR systems.[137] For example, New Hampshire's law prohibits the use of ALPR cameras and other systems that can determine "the ownership of a motor vehicle or the identity of a motor vehicle's occupants on the public ways of the state."[138] However, cameras are allowed for use in the operation of a toll collection system and when related to the monitoring of a structure under the control of the state.

Arkansas follows a less restrictive approach, which disallows the use of license plate cameras by public and private agencies but permits the system to be employed by the police for ongoing investigations, by parking enforcement entities, or for regulating access to secured areas.[139] The statute also allows law enforcement to keep the data for up to 150 days unless it is part of an ongoing investigation.[140]

Other jurisdictions, such as Minnesota, only permit the use of its own license plate database. However, a law enforcement agency may utilize additional sources if the matter relates to an active criminal investigation.[141] That data must be destroyed within thirty days unless the data is related to a criminal investigation. Utah does not allow data to be stored for more than twenty-one days.[142] Montana's statute provides that information gained by a license plate reader may only be used for official law enforcement purposes to identify vehicles that are believed to be: stolen; linked to a wanted, missing, or endangered individual; registered to someone against whom there is an outstanding warrant; in violation of commercial trucking laws; involved in specific criminal surveillance; part of a major crime or incident; or in the vicinity of a recent crime and may

129. *Id.*
130. *Id.*
131. *Id.*
132. *Id.*
133. *Id.*
134. *Id.*
135. *Id.*
136. *Id.*
137. Fisher, *supra* note 94, at 343.
138. *Id.*
139. *Id.*
140. *Id.*
141. MINN. STAT. §13.824 3(b) (2015).
142. MAINE REV. STAT. §2117-A(5) (2013).

be connected to that offense.[143]

On the other hand, Florida's law merely provides that an ALPR refers to high-speed cameras combined with computer algorithms to convert pictures of license plates into computer-readable data. In turn, the Department of State, in consultation with the Department of Law Enforcement, is tasked with creating a schedule for keeping records containing pictures and data obtained through its system. This retention must create a maximum time that the records may be retained.[144]

Despite the various statutory limitations on the use of ALPRs, courts may not automatically suppress evidence or an arrest just because the ALPR statute is not strictly followed or if system guidelines are not properly followed. In *People v. Davila,* the Supreme Court of New York in Bronx County noted that the New York City Police Department uses an image-processing technology system mounted on the top of police cars to automatically identify vehicles by their license plates.[145] The plates are then compared against a "hotlist" containing information about vehicles that have been reported stolen, where registration or insurance coverage has lapsed, or other similar violations of law.[146] If there is a match, an alarm sounds on the laptop computer mounted in the vehicle, notifying the officer of the problem.[147]

NYPD guidelines consisted of a two-step process to safeguard the reliability of license plate reader information. Initially, officers were required to update the hotlist database with information from the last twenty-four hours.[148] If the alarm sounded, before "initiating any law enforcement action", the officer had to look at the database to make sure that the plate reader information is correct.[149] In *Davila*, the officer was driving around in his patrol car but had not verified whether the hotlist had been updated. A car then passed his cruiser and an alarm sounded indicating that the car's registration had been suspended.[150] The officers approached the car and thought that the occupants were acting suspiciously. One law enforcement agent saw a bulge in the defendant's trouser area and found a gun.[151] Upon questioning, the defendant claimed that he had been in an earlier confrontation. After his arrest, the accused moved to suppress the evidence related to the weapon.[152] The court

143. MONT. CODE ANN. § 46-5-117(2)(d)(v) (2017).

144. FLA. STAT. ANN. § 316.0778(2) (West 2014).

145. People v. Davila, 901 N.Y.S.2d 787, 788 (Sup. Ct. 2010).

146. *Id.* at 789.

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id.* at 790.

151. *Id.*

152. *Id.*

denied the motion and found that the officer's failure to follow the guidelines did not invalidate the police stop.[153] According to the court, the NYPD guidelines are merely suggestions for ideal practices and they do not represent the law. The officer reasonably relied on the license plate reader's hotlist and the database was not "stale," as the defendant suggested. Rather, it had been updated only 36 hours before the stop and accurately reflected the status of the owner's car.[154]

Whether scanned license plate data is discoverable was at issue in *American Civil Liberties Union Foundation of Southern California v. The Superior Court of Los Angeles County*.[155] The American Civil Liberties Union ("ACLU") filed suit to obtain the ALPR data collected by the Los Angeles Police Department for one week to ascertain if it showed whether the police were using the information to target specific people, neighborhoods, or organizations as well as to determine the degree to which the technology was threatening individual policy interests.[156] The City objected to the request, claiming that the law allowed it to withhold records that are part of an investigation as well as when the public's interest in disclosure is outweighed by the need to keep the information private.[157] The Supreme Court of California agreed with the City's position and prohibited the discovery of the data. The court noted that the police department recorded between 1.7 and 1.8 million license plates a week and kept that data for two years.[158] Disclosing such material would threaten the privacy of everyone affiliated with the scanned plates and the sheer volume of material would make that threat significant.[159] That data would show the daily activities of its citizens, such as where they were at a certain time, their employment location, home address, and places that they visited.[160] Therefore, the court ruled that the request was a situation in which the "public interest in preventing such a disclosure, clearly outweighs the public interest served by disclosure of these records."[161]

Carpenter v. United States warrants watching in the future because of the potential impact of the decision involving surveillance conducted in public areas.[162] This case dealt with whether the "government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past

153. *Id.* at 791.
154. *Id.*
155. Am. Civil Liberties Union Found. v. Super. Crt., 3 Cal. 5th 1032 (Cal. 2017).
156. *Id.* at 1043-44.
157. *Id.* at 1044.
158. *Id.* at 1037.
159. *Id.* at 1044.
160. *Id.*
161. *Id.*
162. Carpenter v. United States, 138 S. Ct. 2206 (2018).

movements."[163] In every instance when a phone connects to a cell site, it creates a time-stamped record dubbed "cell-site location information (CSLI)."[164] Wireless carriers retain CSLI for the start and end of incoming calls and gather site information from the transmission of text messages and regular data connections.[165]

Carpenter dealt with an incident in 2011 where four individuals were apprehended as suspects in the robbery of several Radio Shack and T–Mobile stores. Based upon a confession, the FBI reviewed the phone records of one of the suspects, and this data and site sector information placed him near the scene of several crimes.[166] He was arrested and moved to suppress the cell-site data provided by the wireless carriers, alleging that the Government's seizure of the records violated the Fourth Amendment because the information had been acquired without a warrant based upon probable cause.[167]

In applying the Fourth Amendment to innovations in surveillance tools, the Court noted that it has sought to "assure preservation of that degree of privacy against the government that existed when the Fourth Amendment was adopted."[168] Because of the huge storage capacity of cell phones, the police must usually acquire a warrant before examining the contents of a phone.[169] The instant fact pattern dealt with the Government's procurement of a wireless carrier's cell-site records revealing the location of the defendant's cell phone whenever he placed or received calls.[170] This personal location information kept by a third party did not fit precisely under any existing precedent so the Court was left to its own devices.[171]

The Court held the use of CSLI constituted a Fourth Amendment violation, noting that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from [the defendant's] wireless carriers was the product of a search."[172] A person does not give up all Fourth Amendment protections merely by entering a public space. Instead, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[173] Allowing

163. *Id.* at 2211.
164. *Id.*
165. *Id.* at 2212.
166. *Id.*
167. *Id.*
168. *Id.* at 2214.
169. *Id.*
170. *Id.*
171. *Id.*
172. *Id.* at 2217.
173. *Id.*

the government to obtain cell-site records violates that expectation.[174] Likewise, mapping a cell phone's position over many days affords an all-encompassing log of the person's whereabouts. This information offers a detailed glimpse into the individual's life, showing his "familial, political, professional, religious, and sexual associations."[175] Since obtaining CSLI constitutes a search, "the Government must generally obtain a warrant supported by probable cause before acquiring such records."[176] The impact of this decision remains to be seen but it does offer safeguards with certain data that is obtained from a public area.

III. POLICE USE OF DRONES

To some, perhaps the ultimate intrusion into one's privacy would occur if the police could take to the air to secretly conduct surveillance of their citizens. That day has arrived with the use of unmanned aerial vehicles ("UAV") or drones. This aerial technology has become commonplace, with 1.1 million UAVs being employed in the United States. It is predicted that this number will triple to almost 3.5 million devices by 2021.[177] The Center for the Study of the Drone at Bard College determined that, as of 2018, as many as 910 state and local public safety agencies have purchased UAVs with more than half of this number belonging to law enforcement agencies.[178]

Police use of drone technology will only increase because of the low cost of the equipment. A good drone costs about $3,000 and it can be equipped with a very powerful zoom-enabled camera for another $3,000. A police helicopter, on the other hand, costs anywhere from one-half million to several million dollars.[179] The cost to fly a helicopter is about $200 to $400 an hour, not counting maintenance expenses.[180] Comparing the costs of these two types of aerial technology, law enforcement could buy a fleet of 500 drones instead of one helicopter. This would allow them to blanket a large area with UAVs that can follow people unnoticed from thousands of feet away and employ software that can identify individuals in an automated fashion.[181]

174. *Id.*

175. *Id.*

176. *Id.* at 2221.

177. Curt Fleming, *Remote Drone Dispatch: Law Enforcement's Future?*, POLICE CHIEF MAG., https://www.policechiefmagazine.org/remote-drone-dispatch/ (last visited Dec. 9, 2019).

178. Jake Laperruque & David Janovsky, *These Police Drones Are Watching You*, POGO (Sep. 25, 2018), https://www.pogo.org/analysis/2018/09/these-police-drones-are-watching-you/.

179. *Id.* at 3.

180. *Id.* at 3-4.

181. *Id.* at 4.

A. UAV and Drone Equipment

Most advances in the development of drones occurred during periods of war.[182] These unmanned flying machines gained much recognition during their use in military incursions in the Middle East following the September 11th attacks. The government employed these devices to perform surveillance in Iraq, Afghanistan, and Iran, in addition to dropping targeted weapons.[183] Because drones fly hundreds of feet above the ground, they are usually undetectable by those being watched.[184] These flying machines gained a domestic application in 2005 when Customs and Border Patrol started using them to monitor the Canadian and Mexican borders, detecting large quantities of marijuana and cocaine.[185]

Surveillance UAVs have very sophisticated imaging technology that offers the capability to acquire detailed images of individuals, terrain, houses and even small objects.[186] The drone cameras are usually high definition and can provide live-feed video streams at a rate of 10 frames a second. Some systems even allow the operator to follow more than 50 varied targets across a distance of 65 square miles.[187] Because the units can be equipped with thermal infrared video cameras, heat sensors, and radar, drones can allow sophisticated and continuous surveillance 24 hours a day.[188] They can also be coupled with cell-phone interception devices, specialized software (such as license plate readers), facial recognition software and GPS trackers.[189]

UAVs come in varying sizes from small quadrotors to large fixed aircraft. They differ from manned aircraft due to their much smaller size, reduced costs, ability to fly at low altitudes and easy deployment.[190] Drones can be manually operated through hand-held devices with video cameras so that the operator can view the area in which the device is being employed. They can fly autonomously without the need for a person to manually control the drone.[191]

182. *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC.ORG, https://epic.org/privacy/drones/ (last visited Dec. 8, 2019).

183. *Id.*

184. *Id.*

185. Jessica Dwyer-Moss, *The Sky Police: Drones and the Fourth Amendment*, 81 ALB. L. REV. 1047, 1048 (2018).

186. Domestic Unmanned Aerial Vehicles (UAVs) and Drones, *supra* note 182, at 2.

187. *Id.*

188. *Drones/Unmanned Aerial Vehicles*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/dronesunmanned-aerial-vehicles (last visited Dec. 9, 2019).

189. *Id.* at 1.

190. *Id.*

191. *Id.*

B. UAV Use by Law Enforcement

Police departments routinely use UAV and drone technology as part of their law enforcement arsenal.[192] This application has moved past the experimental phase and drones are being employed by law enforcement in their day to day operations at a rapidly increasing pace. This usage has increased by a staggering 518% just during the past two years.[193]

A variety of police drone applications exist, ranging from search and rescue operations to crime scene analysis.[194] For example, UAVs permit the police to scour a location where suspects might be hiding while keeping the surveillance as discreet as possible. Where police vehicles can be easily spotted, a drone permits discreet observations while safeguarding officers from danger.[195] UAVs are very useful in search and rescue missions because they can cover vast territories more quickly and efficiently than officers on foot. They can also fly under trees, over water, and between buildings—providing access that is not possible by a chopper.[196] Drones are even employed to help the police follow a suspect. For instance, it is difficult for ground forces to keep track of a suspect who has fled to a rooftop area. A UAV provides an eye in the sky that relays key information about a suspect's movements and directs the police to optimal positions.[197] Aerial devices can also help identify suspects, ascertain what weapons they might be carrying, and assist in collecting evidence that may be impossible to retrieve from the ground.[198]

Other applications include using a drone to obtain a three-dimensional reconstruction of an accident scene, since the aircraft can obtain evidence from angles that would normally be impossible to film without a helicopter.[199] UAVs are used to manage and observe traffic and to determine why it is backed-up. This information can then be used to detour traffic, change the rate of red and green lights to better manage the flow of traffic, and detect speeding vehicles.[200] Drones also have applications following a natural disaster where it may be impossible for vehicles to access the area and identify people in need of help. They have

192. *5 Ways Drones Benefit Police*, DRONE USA (Nov. 16, 2018), https://www.droneusainc.com/articles/5-ways-drones-benefit-police.

193. *Id.* at 2.

194. *Id.*

195. *Id.* at 3.

196. Derek Wheeler, *Police Drones (UAVs)*, DSLR PROS, https://www.dslrpros.com/police-drones.html (last visited Dec. 8, 2019).

197. Stephen Rice, *10 Ways That Police Use Drones to Protect and Serve*, FORBES (Oct. 7, 2019), https://www.forbes.com/sites/stephenrice1/2019/10/07/10-ways-that-police-use-drones-to-protect-and-serve/#e69d6f165806.

198. *Id.* at 2.

199. *Id.*

200. *Id.* at 4.

even been deployed to manage large events such as the Super Bowl, Spring Break parties, and the Daytona 500. This surveillance allows the police to detect trouble before it becomes unmanageable and to redirect their personnel to troubled areas.[201]

A recent trend in drone use arises in a business context. A growing number of employers are utilizing UAVs to oversee their property and workers on a customary basis.[202] These applications include watching workers believed to be engaged in the theft or misappropriation of confidential information, viewing the performance and efficiency of workers, and halting unsanctioned use of, or damage to, business assets.[203]

C. Autonomous UAVs

There has been much publicity about industries, such as Amazon, attempting to expand the commercial application of autonomous drones by delivering their products. There are three major roadblocks to this adoption in the United States: Federal Aviation Administration ("FAA") rules, limited flight time, and privacy concerns.[204] The FAA has two regulations that are obstacles to the full implementation of autonomous drone operation: Beyond Visual Line of Sight ("BVLOS") flight, and Detect and Avoidance ("DAA").[205] BVLOS rules provide that an operator must be able to visualize the drone at all times while in flight. This directive would prevent autonomous or remotely directed flights. The pilot provides a manned aircraft with a built-in system to detect other planes in the area and to take avoidance measures when necessary. This is difficult with a drone because the operator is on the ground, or, in the case of an autonomous UAV, no pilot exits to "see and avoid" other aircraft by taking evasive action.[206] The second obstacle is that current battery limitations provide drones with an average flight life of about 30 minutes.[207] The last hurdle is one of privacy and the drone's ability to visualize areas that are normally not accessible to public view.[208]

201. *Id.* at 6.

202. Charlie Plumb, *Drones in the Workplace: Tips for Handling New Technology*, 24 No. 1 Okla. Emp. L. Letter 3, January 2016.

203. *Id.* at 1.

204. Fleming, *supra* note 177, at 2.

205. *Id.*

206. *Id.*

207. *Id.*

208. *Id.*

D. Criticisms of UAV and Drone Technology

Critics maintain that aerial surveillance undercuts the safeguards imposed to prevent unreasonable location tracking and the government's accumulation of personal information.[209] Drones present a unique challenge for privacy rights.[210] They provide the government with the opportunity to track the movements of individuals and index participation in constitutionally protected activities such as protests, political rallies, and religious ceremonies.[211] After all, inconspicuous drones permit the police to spy on people from thousands of feet away with a high degree of precision.[212] Coupled with other automated identifying technologies, such as license plate readers and facial recognition software, Big Brother will be able to surveil people unnoticed, monitor their movements over time, and identify them through a single image.[213]

These concerns are real, as demonstrated by research conducted by the ACLU. The ACLU discovered that the FBI was using aerial surveillance to record protestors, and sellers of the equipment were marketing drones to law enforcement agencies by highlighting the drone's capacity to identify people at public gatherings.[214] Drone cameras can even be paired with facial recognition software contained in the FBI's Next Generation identification database or DHS' IDENT, two of the biggest compendia of biometric data in the world, thereby creating First Amendments perils for political protestors.[215]

E. Judicial and Legislative Responses to UAV and Drone Technology

UAVs usually operate in an area below the navigable airspace regulated by the FAA, "in the vertical curtilage that is viewed as belonging to a property owner."[216] This airspace was unregulated until recently. Now, these unmanned aircraft trigger FAA law requirements, as well as the property rights of landowners.[217] In this regard, the government, in June 2016, issued its first operational rules for customary use of small, unmanned aircraft systems. The regulations provide safety rules for drones that weigh less than fifty-five pounds and conduct non-

209. Laperruque, *supra* note 178, at 2.

210. Domestic Unmanned Aerial Vehicles (UAVs) and Drones, *supra* note 182.

211. Laperruque, *supra* note 178, at 2.

212. *Id.* at 3.

213. *Id.*

214. *Id.*

215. Domestic Unmanned Aerial Vehicles (UAVs) and Drones, *supra* note 182.

216. Elizabeth Austermuehle, *Drones and Private Property Rights*, 34 No. 26 WESTLAW J. AVIATION, 1 (2017).

217. Domestic Unmanned Aerial Vehicles (UAVs) and Drones, *supra* note 182.

hobbyist operations.[218]

Generally, UAV operators are required to fly their devices within their visual sightline and regulations bar them from flying over individuals on land who are not participating in the drone's operation.[219] This dramatically restricts drone use over land that does not belong to the UAV's operator, but regulations do not expressly address the rights of adjacent landowners who desire to limit drones from flying over their property.[220] In the absence of federal or state laws permitting these unmanned aircraft to operate above private property without the owner's consent, drones are not authorized to fly over these areas.[221] Violators are subject to suit by landowners who may enforce their rights through a tort action, including trespass and invasion-of-privacy claims.[222]

In a criminal context, the Supreme Court of the United States has found that citizens generally do not enjoy Fourth Amendment protections against drone use because anyone might see what can be visualized from the air.[223] The weakness in this position is that the average person does not use drones with the sophistication of those employed by the government.[224] State courts have also issued varying opinions on whether UAVs violate a person's privacy rights.[225]

Most jurisdictions do not require the police to obtain a search warrant before engaging in drone surveillance. However, at least eighteen states now require law enforcement in certain situations to obtain a warrant before using a drone for surveillance purposes, while others have issued civil penalties if drones take video or sound recordings of another without obtaining that person's consent.[226] These jurisdictions include Alaska, Florida,[227] Idaho, Illinois,[228] Indiana, Iowa, Maine,[229] Montana, North Carolina,[230] North Dakota,[231] Oregon, Tennessee,[232] Texas,[233] Utah,[234]

218. *Id.*
219. *Id.*
220. *Id.*
221. *Id.*
222. *Id.*
223. Austermuehle, *supra* note 216, at 4.
224. *Id.*
225. *Id.*
226. Laperruque, *supra* note 178 ; CAL. CIV. CODE § 1708.8 (West 2016).
227. FLA. STAT. ANN. § 934.50 (West 2017).
228. 20 ILL. COMP. STAT. 5065/1-99 (West 2017) (repealed 2017).
229. ME. REV. STAT. ANN. tit. 25, § 4501 (2015).
230. 2013 N.C. Sess. Laws 41.
231. N.D. CENT. CODE ANN. § 29-29.4-02 (West 2015).
232. TENN. CODE ANN. § 39-13-903 (West 2019).
233. TEX. GOV'T. CODE ANN. §§ 411.062, §423.002(a), §423.0045 (West 2019).
234. UTAH CODE ANN. § 72-14-101 (West 2017) (original version at § 63g-18-101).

Vermont, Virginia[235] and Wisconsin.[236]

The first judicial pronouncements involving aerial surveillance arose with searches conducted by traditional aircraft. In 1986 in *California v. Ciraolo*, the Supreme Court determined that a search of a fenced-in backyard conducted by air and without a warrant was allowed under the Fourth Amendment. [237] The facts reveal that based upon a tip that marijuana was being grown in the defendant's secured backyard, a private airplane was flown over the premises and an officer spotted the illegal plants growing in the backyard.[238] The police obtained a search warrant and seized the plants. The defendant filed a motion to suppress evidence of the seizure, claiming that aerial surveillance was a violation of his Fourth Amendment rights.[239] The Court noted that the defendant had the subjective intent to maintain his privacy since a ten-foot-high fence had been built around the backyard to conceal the marijuana crop.[240] However, such a fence does not hide these illegal plants from police observation by an officer standing on top of a truck or bus.[241] After all, the Fourth Amendment does not protect a person's expectation of privacy if the officer's observations can be made from a public viewing point.[242] In this case, the observations of the marijuana occurred within public airspace. Society is operating in an era where aircrafts routinely fly over property, so it is not reasonable to conclude that marijuana plants in someone's backyard are constitutionally protected.[243] The police are not mandated to obtain a warrant when they use public airways at an altitude of 1,000 feet to see what is visible to the naked eye.[244]

The Supreme Court decided a second case during the same year in *Dow Chemical Company v. United States*.[245] Dow Chemical employed elaborate measures to safeguard its property from the prying eyes of those on the ground.[246] Under a plant inspection, the Environmental Protection Agency ("EPA") hired a commercial aerial photographer to shoot a picture of the plant from various altitudes.[247] Dow maintained that these

235. VA. CODE ANN. § 19.2-60.1 (West 2019).

236. *See Drone Laws By State*, CONSUMER.FINDLAW.COM (Mar. 28, 2019), https://consumer.findlaw.com/consumer-transactions/drone-laws-by-state.html; Laperruque, *supra* note 178.

237. California v. Ciraolo, 476 U.S. 207 (1986).

238. *Id.* at 207.

239. *Id.*

240. *Id.* at 211.

241. *Id.*

242. *Id.* at 213.

243. *Id.*

244. *Id.* at 215.

245. Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

246. *Id.* at 227.

247. *Id.*

pictures violated its Fourth Amendment rights by exposing trade secrets.[248]

The Court started its decision by noting that Dow admitted that an aerial observation with the naked eye, or the snapping of a picture from a surrounding hill overlooking the facility, would not be constitutionally protected.[249] The issue was whether an aerial mapping camera of a large industrial plant was permissible under the Fourth Amendment.[250] In this regard, the Court has noted that "the public and police lawfully may survey lands from the air."[251] The pictures, in this case, were not so detailed as to raise Fourth Amendment concerns. Although the images indeed provided the EPA with "more detailed information than naked-eye views, they remain limited to an outline of the facility's buildings and equipment. The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[252]

A third case reached the Supreme Court a few years later in *Florida v. Riley*.[253] The issue before the Court was "[w]hether surveillance of the interior of a partially covered greenhouse in a residential backyard from the vantage point of a helicopter located 400 feet above the greenhouse constitutes a 'search' for which a warrant is required under the Fourth Amendment."[254] The Court found that this search did not violate the Constitution based upon its prior holdings. The judges were not impressed by the low altitude at which the helicopter flew while making the observations, since any member of the public flying in an aircraft could have made the same observations.[255] While these cases do not specifically address the framework of surveillance conducted by a drone, they set the foundation for the subsequent law in this area.

Westlaw searches involving drones and the Fourth Amendment or drone surveillance by the police reveal only a handful of cases on the topic. Several of the decisions involve pro-se plaintiffs.[256] *Byers v. State of Indiana* is a recent decision involving a woman who was mowing her lawn when she discovered a drone in her backyard.[257] She noticed a flash drive attached to the unmanned aircraft, so she pugged it into her home

248. *Id.* at 232.

249. *Id.* at 234.

250. *Id.*

251. *Id.* at 238 (citing Oliver v. United States, 466 U.S. 170, 179 (1984)).

252. *Id.*

253. Florida v. Riley, 488 U.S. 445 (1989), *reh'g denied*, 490 U.S. 1014 (1989).

254. *Id.* at 447-48 (citing Riley v. State, 511 So. 2d 282 (Fla. 1987), *cert. granted, rev'd*, 488 U.S. 445 (1989)).

255. *Id.* at 450-51.

256. This statement is based upon a Westlaw search conducted by the author on December 19, 2019.

257. Byers v. State, 134 N.E.3d 1051 (Ind. Ct. App. 2019), *transfer denied*, 141 N.E.3d 807 (Ind. 2020).

computer and found footage of a woman, who she recognized as her neighbor, handling a bag filled with white powder.[258]

The homeowner contacted the police and turned over the flash drive, and the police then obtained a search warrant. A subsequent search of the defendant's home uncovered methamphetamine and a handgun.[259] The defendant was arrested and she moved to suppress the evidence obtained as the result of the drone search under the Fourth Amendment.[260] The Court found the evidence was admissible since only four days had elapsed from when the video was shot and the issuance of the warrant.[261] At no time did the defendant directly challenge the video obtained by the drone.

People have also been arrested for using drones to take unauthorized images. For example, one of the first prosecutions for conducting unauthorized surveillance through the use of a drone occurred in New York when the defendant was arrested after taking images of a medical building using his unmanned device.[262] At trial, the defendant claimed that he was using his device to take "videos and photos of the facade of the structure" while waiting for his mother's doctor's appointment to finish.[263] The defendant asserted that the drone's camera did not have a zoom lens, the building's windows were tinted, and the video did not reveal the inside of the premises. [264] Both the government and workers inside of the office raised concerns about patient privacy, but the defendant was found not guilty of the charges. [265]

The opposite result was rendered in Wisconsin in 2015.[266] In this case, a drone operator was found guilty of five counts for the employment of his unmanned aircraft "to harass residents in a…neighborhood."[267] The facts show that the charges were filed in response to complaints by neighbors that a drone was "flying near their windows and observing them on their private property."[268] The defendant was convicted of violating a law that made it illegal for an "individual to use a drone to observe a person in a place where that person should have a reasonable expectation of privacy."[269]

258. *Id.* at 1053.
259. *Id.*
260. *Id.* at 1054.
261. *Id.* at 1056.
262. Rebecca L. Scharf, *Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy*, 94 IND. L.J. 1065, Summer 2019, at 1067.
263. *Id.*
264. *Id.*
265. *Id.*
266. *Id.*
267. *Id.*
268. *Id.* at 1067-68.
269. *Id.* at 1068.

Issues involving drone use have arisen in a civil context. *F.W.T. v. F/T.* provides an example.[270] This case entails a dispute between a father and son concerning a long-standing quarrel between them.[271] The purpose of the lawsuit was an action by the son to obtain an order against harassment because his father allegedly had someone fly a drone over his property three times to hinder the son's development of the land.[272] According to the law, such an action requires a showing that the conduct "caused fear, intimidation, abuse or damage."[273]

The court refused to grant the protective order and noted that there was no evidence to show that the elements of the statute had been satisfied.[274] Merely flying a drone over, or trespassing upon, the land to film a worksite does not rise to the level of harassment within the meaning of the law.[275] In no way did the court approve of the conduct of the father, but it noted that the proper cause of action would have been a claim for "nuisance, trespass or other cause of action, enforceable through" equitable relief.[276]

Flores v. State of Texas presented a constitutional challenge to a recently passed law regulating the utilization of drones.[277] The evidence demonstrated that drones have become increasingly popular by law enforcement agencies for policing and surveillance activities.[278] This use has also expanded into the public sector for commercial, scientific and recreational purposes. This has raised questions about privacy rights and the legal use of drone-captured pictures.[279] In this regard, Texas passed a law making it criminal to use a drone to take images of other individuals on their land. It further allowed the property owner to obtain injunctive relief or monetary damages in case of a violation.[280] The police, however, enjoy an exception when they use drones for official activities, such as the pursuit of a suspect, documenting a crime scene or taking pictures for immigration purposes within twenty-five miles of the border.[281]

The plaintiff, in this case, was a resident of Laredo, Texas and his property was within the twenty-five-mile zone. He filed suit to obtain injunctive relief declaring that the border exception violated his rights

270. F.W.T. v. F.T., 101 N.E.3d 336 (Mass. App. Ct. 2018).
271. *Id.* at 338-39.
272. *Id.*
273. *Id.* at 339 (citing Seney v. Morhy, 3 N.E.3d 577, 582 (Mass. 2014)).
274. *Id.* at 339.
275. *Id.* at 340.
276. *Id.* at 340, n.8.
277. Flores v. State of Texas, No. 5:16-CV-130, 2017 WL 1397126 (S.D. Tex. Mar. 31, 2017).
278. *Id.* at *1.
279. *Id.*
280. *Id.*
281. *Id.*

under the Equal Protection Clause and the right to privacy afforded by the Constitution.[282] As the plaintiff noted, this exception provides a "playground for drone enthusiasts who would otherwise be precluded from filming people in their homes, washing their cars, gardening in their yard, or simply walking on their private property" to be observed without any type of protection as long as they are within twenty-five miles of the border, while everyone else in the state is protected.[283] The court denied the request on the basis that the plaintiff lacked standing to challenge the law. It noted that standing requires more than an allegation of residency within the zone.[284] The plaintiff must show that an identifiable drone was used to take images of him on his land. Mere generalizations and a hypothetical injury are not enough[285] and living within the twenty-five miles zone was insufficient to establish an actual injury.[286]

In *Allums v. Department of Homeland Security*, a pro se plaintiff claimed that the government was harassing him through a variety of activities, such as showing up at his house to eat ice cream and stare at him, as well as committing copyright violations of his work.[287] In his fifth count, Allums asserted that he had been the subject of drone surveillance and attacks by the government, as well as agents telling him that he would soon be "killing Americans with Drone Airplanes."[288] The plaintiff maintained that these activities were carried out by agents who ordered his execution by airborne devices that flew close to his head, causing him to duck and fall to the ground.[289] Not surprisingly, the court dismissed the lawsuit for the failure to state a claim. The court considered the plaintiff's allegations fanciful and frivolous. There were simply no facts to support his conclusory allegations that the government was surveilling him.[290]

IV. FACIAL RECOGNITION SOFTWARE

Anonymity in the 21st Century is no longer an option since most people now have some form of photo identification and surveillance technology is constantly expanding. These developments have caused most members of society to have had an encounter with facial recognition software

282. *Id.*

283. *Id.*

284. *Id.* at *4.

285. *Id.* at *3.

286. *Id.*

287. Allums v. Dep't of Homeland Sec., No. 13-cv-00807 JSC, 2013 WL 4426258, at *1-2 (N.D. Cal. Aug. 14, 2013).

288. *Id.* at*3.

289. *Id.*

290. *Id.* at *6; *see also* Strong v. United States, No. 11CV2957 JLS (WVG), 2012 WL 202780 (S.D. Cal. Jan. 23, 2012).

without their knowledge or consent. Facial recognition software refers to equipment that has the dual role of "connecting faces to identities" and enabling the "distribution of those identities across computer networks."[291]

Facial recognition technology ("FRT") can be traced back to the mid-1960s, when researchers first started working with computers to recognize human faces.[292] By the 1990s, automated facial recognition algorithms were developed, and after the September 11th attacks, FRT became part of the public discourse.[293] The federal government invested heavily in FRT, and millions of dollars in grants were awarded to state and local governments to establish databases. What started as government-funded research in computer sciences eventually made its way into the private sector.[294] FRT software is now employed by stores to scan the faces of customers and pre-identify shoplifters and people known to file lawsuits.[295] Some airlines use FRT to speed up the boarding process.[296] Microsoft has even created a billboard that recognizes people as they walk by and then deploys personalized ads associated with the individual's buying history.[297]

FRT is linked to a database of images, such as mugshots, government issued identification photos (such as drivers licenses and passports), and social media accounts to rapidly identify people through biometrics to match key facial features, such as the distance between the eyes and the gap between the forehead and chin.[298] These measurements then create a "facial signature" that is linked to a mathematical formula and compared to a database of stored images.[299] As one might imagine, FRT is a much in-demand law enforcement tool for solving crimes by ascertaining the identity of the offenders who are imaged on surveillance footage, locating

291. Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* 15 (N.Y. Univ. Press, 2011).

292. Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS 1, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm (last visited Feb. 7, 2020).

293. Gates, *supra* note 292, at 27 (noting that proponents of FRT suggested that this technology could have prevented the hijackings).

294. *Id.*

295. Ben Sobel, *Facial Recognition Technology is Everywhere. It May Not be Legal*, WASH. POST (June 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/?arc404=true.

296. Francesca Street, *How Facial Recognition is Taking Over Airports*, CNN (Oct. 8, 2019), https://www.cnn.com/travel/article/airports-facial-recognition/index.html.

297. *Id.*

298. Nicole Martin, *The Major Concerns around Facial Recognition Technology*, FORBES (Sept. 25, 2019), https://www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#235792e84fe3.

299. *Id.*

fugitives in a crowd, or locating terrorists as they enter the country.[300] Other suggested applications include spotting problem gamblers in casinos, greeting guests at hotels or on ships, linking people on dating websites, identifying underage drinkers, and helping take attendance at schools.[301]

A. How Does FRT Work?

Some people have the innate ability to remember a face. This recognition occurs because the individual can retain identifying information about the facial features such as the eyes, nose, mouth, and how those features come together to form a familiar pattern.[302] Facial recognition systems work similarly, albeit on an algorithmic scale. Where a person visualizes a face, FRT recognizes data that is stored and can be easily accessed. In this regard, 50% of adults in the United States have their pictures warehoused in one or more facial-recognition databases that law enforcement agencies can search.[303] Matching a picture to a person generally works in the following way:

- The first step requires that a person's face be captured.[304] Traditionally, this mandates the captured picture to be of a face looking directly at the camera, with only a slight change in light or facial expression from the database image.[305]
- A template for FRT is then made, which consists of measurements of facial characteristics, such as the distance between the eyes, the width of the mouth or depth of the eye sockets. These landmarks are dubbed nodal points, and the measurements are inputted into a template with a distinctive code.[306] Every face has about 80 nodal points.[307]
- These nodal points are then analyzed, and the software will compare the template of the person's face to those stored in a database to search for a potential match.[308]

300. Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will it Take Us?*, A.B.A., https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ (last visited Feb. 6, 2020).

301. *Id.*

302. Steve Symanovich, *How Does Facial Recognition Work?*, U.S.NORTON.COM, https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html (last visited Feb. 7, 2020).

303. *Id.*

304. *Id.*

305. Bonsor, *supra* note 293, at 2.

306. Symanovich, *supra* note 303.

307. Bonsor, *supra* note 293, at 2.

308. Hamann, *supra* note 301.

The chances of law enforcement officials finding a match are high since more 117 million Americans have facial pictures stored in one or more government databases and the FBI has access to 412 million images.[309] In fact, FBI facial recognition searches now outnumber court-ordered wiretaps.[310]

B. Advantages of FRT

FRT has multiple applications and offers a variety of benefits that vary depending upon the user. For instance, governments internationally use FRT in police, military, and intelligence operations, and businesses use FRT in security, advertising, banking, sales, and health care.[311] One of FRT's most important benefits, however, is that it can make law enforcement operations much more efficient.

Officials can submit a photograph of a recently apprehended individual through its system to identify the person and ascertain if there are outstanding warrants for other offenses.[312] It can help officers in the field observing a large gathering, like a sporting event or political rally, identify people of interest, known terrorists, and wanted criminals.[313] It is also being used to ensure efficient regulation. The New York Department of Motor Vehicles, for instance, has used FRT to detect fraudulent licenses[314] and the Pinellas County Sheriff's Office in Florida uses it to identify inmates at the time of booking and release.[315]

FRT offers a faster way to process individuals without stopping each person to ask for identification. The system can even be used as an alternative for a password to access computers[316] or to gain entry into a building or secured location. Since no passwords are needed with facial recognition, there is nothing that a hacker or thief could compromise. This would prevent someone from using a stolen identification for

309. Symanovich, *supra* note 303.

310. Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, PERPETUALLINEUP.ORG 2 (Oct. 18, 2016), https://www.perpetuallineup.org/background.

311. Ashley Deeks & Shannon Togawa Mercer, *Facial Recognition Software: Costs and Benefits*, LAWFARE (Mar. 27, 2018), https://www.lawfareblog.com/facial-recognition-software-costs-and-benefits.

312. *Id.*

313. *Id.* at 1-2.

314. Anthony M. Carter, Facing Reality: The Benefits and Challenges of Facial Recognition for the NYPD 58 (Sept. 2018) (unpublished M.A. thesis, Naval Postgraduate School) (available online), https://www.hsdl.org/?view&did=818128.

315. *Id.*

316. *6 Benefits of Facial Recognition Everyone Should Know*, Tech. BUS. GUIDE, https://techbusinessguide.com/benefits-facial-recognition-everyone-should-know/ (last visited Feb. 10, 2020).

impersonation purposes.[317] It is also favored over fingerprint scanning due to its non-contact process. The possible disadvantages of dealing with fingerprint identification methods, such as germs or smudges, will be eliminated.[318] It can even eliminate time fraud by employees. Facial recognition will prevent a co-worker from time-stamping someone else's attendance or timesheets since each person must pass a face-scanning device to check in and out of work.[319]

A lesser-known advantage of FRT is its ability to find missing persons. For instance, police in China were able to find a missing six-year-old by using a picture that had been taken days earlier with cameras linked to FRT.[320] New Delhi authorities reported finding nearly 3,000 missing children within days of launching a facial recognition program.[321] Aside from leading to breakthroughs in missing children cases, FRT has also led to breakthroughs in cases involving the mentally ill. For instance, a mentally ill man who had been in a Chinese hospital for over a year was reunited with his family. The hospital had been unable to identify him, but a facial recognition firm was able to do so by linking a picture of his face with public records.[322] These success stories suggest that FRT could be an essential tool in helping vulnerable populations.

C. Technological Limitations of FRT

FRT has certain limitations. This was revealed following the Boston Marathon bombings, which showed that the FBI lacked the appropriate software and databases to immediately identify the suspects.[323] While government databases contained the pictures of both Boston Marathon bombings suspects, the software could not match the surveillance footage to these database images.[324] Although FRT has become increasingly accurate, certain factors will still yield false positives, false negatives, or, as in this case, undetected faces.[325] These influences include the sophistication of the camera, distance, database size, algorithm, and

317. *Id.*

318. *PROS AND CONS OF FACIAL RECOGNITION TECHNOLOGY*, RTI, HTTPS://WWW.1RTI.COM/PROS-CONS-OF-FACIAL-RECOGNITION-TECHNOLOGY/ (LAST VISITED FEB. 10, 2020).

319. *Pros and Cons of Facial Recognition Technology for Your Business*, UPWORK (Dec. 27, 2017), https://www.upwork.com/hiring/for-clients/pros-cons-facial-recognition-technology-business/.

320. Carter, *supra* note 315.

321. Rob Watts, *Facial Recognition as a Force of Good*, BIOMETRIC TECH. TODAY, March 2019.

322. Anthony Cuthbertson, *Facial Recognition Technology Reunites Lost Man with His Family*, INDEP. (Apr. 19, 2018), https://www.independent.co.uk/life-style/gadgets-and-tech/news/facial-recognition-reunite-family-man-lost-china-tech-mental-health-a8312161.html.

323. Jeffrey Edgell, *Four Limitations of Facial Recognition Technology*, FED TECH (Nov. 22, 2013), https://fedtechmagazine.com/article/2013/11/4-limitations-facial-recognition-technology.

324. *Id.*

325. Carter, *supra* note 315.

the subject's race and gender.[326]

There are several limitations to FRT. Poor image quality will limit the effectiveness of FRT since it affects the usefulness of facial-recognition algorithms. This is an inherent problem because the quality of a scanning video is much lower than that of a digital camera.[327] The comparative dimensions of the face with the image size also influence how well the face will be identified. Therefore, small image sizes cause facial recognition difficulties.[328] The angle of the target's face to the camera is another factor that significantly impacts the recognition score. The more direct the face is to the camera, the higher the resolution of the image becomes, and a higher score is achieved for a resulting match. Accuracy rates also drop as the number of pictures in a database increases. This is because the database is likely to have images of people that look very similar, leading the algorithm to pick the wrong person.[329]

The accuracy of automated facial recognition algorithms also depends upon the subject. The faces of individuals change over time, which can throw off the algorithm in identifying a person from an earlier picture. Additionally, changes that happen from one day to the next, such as hairstyles and facial expressions, can lead to improper identification.[330] Finally, accuracy rates are lower in certain demographics. Facial recognition algorithms have been less successful with minorities, women, and young adults than Caucasians, men, and older adults.[331] This is because facial-recognition algorithms were trained on databases that mostly contained pictures of white males.[332] As a result, one study found that there is an error rate of around 31% when identifying the gender of women with dark skin.[333]

Accuracy is important when a person's civil and liberty interests are involved, which is why FRT vendors advertise accuracy rates of over 95%.[334] However, this figure must be questioned when it is followed by

326. Jake Laperruque, *Unmasking the Realities of Facial Recognition,* POGO (Dec. 5, 2018), https://www.pogo.org/analysis/2018/12/unmasking-the-realities-of-facial-recognition/.

327. Edgell, *supra* note 324.

328. *Id.*

329. *See* Garvie et al., *supra* note 311. (noting that sixteen states allow the FBI to access their driver's license and ID databases).

330. Hamann & Smith, *supra* note 301.

331. Garvie et al., *supra* note 311.

332. *See* Jieshu Wang, What's in Your Face? Discrimination in Facial Recognition Technology, 30 (Apr. 13, 2018) (unpublished M.A. thesis, Georgetown University) (available online), https://repository.library.georgetown.edu/bitstream/handle/10822/1050752/Wang_georgetown_0076M_14043.pdf?sequence=1&isAllowed=y ("It is estimated that in one widely used FRT training dataset, 75% are male, and over 80% are white.").

333. *The Limits of Facial Recognition Technology*, NEW HUMANIST (Feb. 18, 2019), https://newhumanist.org.uk/articles/5419/the-limits-of-facial-recognition-technology.

334. Edgell, *supra* note 324.

the disclaimer: "[This company] makes no representation or warranties as to the accuracy and reliability of the product in the performance of its facial recognition."[335] Even less reassuring is the fact that law enforcement is not required to perform independent testing to determine the accuracy of the FRT it uses.[336] While the National Institute of Standards and Technology ("NIST") conducts voluntary tests of FRT every four years, many law enforcement entities do not participate in these audits.[337] Some law enforcement entities recognize that FRT is not flawless, so they have a human verify the results.[338] However, this additional step does not guarantee accuracy, since people tend to be good at recognizing familiar faces but have difficulty recognizing unfamiliar faces.[339] Inaccuracies are equally prevalent in the private sector.

D. Legislative Responses to FRT

Some legislatures have passed laws that limit the use of FRT and courts have interpreted these laws to require warrants and other protections.[340] However, Congress has yet to enact federal legislation that directly regulates FRT. This is a major concern among citizens because of questions about the technology's accuracy and whether there is built-in bias and misinformation in these systems.[341] Nevertheless, FBI facial recognition systems are governed primarily by two statutes: the Privacy Act of 1974[342] and the E-Government Act of 2002.[343] These statutes require that the FBI conduct Privacy Impact Assessments ("PIA"s) of its biometric programs and that it employ Fair Information Practices Principles ("FIPPS").[344] PIAs analyze how personal identifiable information is handled in electronic systems and determine the risk of

335. *Id.*

336. Clare Garvie & Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, ATLANTIC (Apr. 7, 2016), https://apexart.org/images/breiner/articles/FacialRecognitionSoftwareMight.pdf.

337. *Id.*

338. John D. Woodward, et al., *Biometrics: A Look at Facial Recognition*, RAND 13, https://www.rand.org/pubs/documented_briefings/DB396.html (last visited Feb. 22, 2020).

339. *Id.* at 11. (explaining that in a British study conducted at a supermarket, 34% of the cards accepted by trained supermarket cashiers had a picture of a person that did not look like the shopper and 7% of the rejected cards contained a picture of the actual shopper).

340. Garvie et al., *supra* note 311.

341. Martin, *supra* note 299, at *2.

342. 5 U.S.C. § 552a (2014).

343. 44 U.S.C. § 101 (1996); 44 U.S.C. § 3501 et seq (2002); Sharon Nakar & Dov Greenbaum, *Now You See Me, Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. SCI. & TECH. L. 88, 105 (2020).

344. *Id.* at 105-06.

collecting, maintaining, and disseminating this information.[345] Meanwhile, FIPPs highlight the importance of transparency, consent, limited use, data quality, data minimization, security, and accountability when dealing with personal identifiable information. [346]

Efforts to implement laws that specifically target FRT use are underway. Last year, the House of Representatives passed an amendment to the Intelligence Authorization Act for the Fiscal Year 2020,[347] which would require that the Director of National Intelligence report FRT use, accuracy, policies, and its potential impact on constitutional rights.[348] Meanwhile, two Senators have introduced the Facial Recognition Technology Warrant Act, which would require federal law enforcement to obtain a warrant to use FRT for tracking the movements of a person for more than three days.[349] Other recently proposed bills include the Algorithmic Accountability Act,[350] the Commercial Facial Recognition Privacy Act,[351] the No Biometric Barriers Act,[352] the FACE Protection Act[353], and H.R.3875.[354] The Algorithmic Accountability Act would require that entities storing personal information conduct impact assessments of their automated decision systems.[355] The Commercial Facial Recognition Privacy Act would prohibit commercial entities from using FRT to identify consumers without their consent.[356] The No

345. *Department of Justice /FBI Privacy Impact Assessments (PIAs)*, FBI, https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments (last visited Feb. 5, 2020).

346. *National Domestic Communications Assistance Center: Executive Board Meeting*, FBI (Sept. 21, 2016), https://ndcac.fbi.gov/file-repository/2016-september-fair-information-practice-principles.pdf/view.

347. *See HPSCI Fact Sheet on H.R. 3494 Fiscal Year 2020 Intelligence Authorization Act*, U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE, https://intelligence.house.gov/uploadedfiles/fact_sheet_on_2020_iaa.pdf.

348. *See* Amendment to Rules Committee (July 15, 2019), https://amendments-rules.house.gov/amendments/JAYAPA_066_xml71519135205525.pdf; *see also Oakland Approves Face Recognition Surveillance Ban as Congress Moves to Require Government Transparency*, ACLU (July 17, 2019), https://www.aclu.org/press-releases/oakland-approves-face-recognition-surveillance-ban-congress-moves-require-government (noting that the ACLU is now urging Congress to vote in favor of this amendment).

349. *See* Facial Recognition Technology Warrant Act of 2019, S.2878, 116th Cong. (2019).

350. *See* Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019).

351. *See* Commercial Facial Recognition Privacy Act of 2019, S.847, 116th Cong. (2019).

352. *See* No Biometric Barriers to Housing Act of 2019, H.R. 4008, 116th Cong. (2019).; Inioluwa Raji et al., *Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing*, *in* PROCEEDINGS OF THE 2020 AAAI/ACM CONFERENCE ON AI, ETHICS, AND SOCIETY 145 (Feb. 2020), *available at* https://arxiv.org/pdf/2001.00964.pdf.

353. *See* FACE Protection Act of 2019, H.R.4021, 116th Cong. (2019).

354. *See* To prohibit Federal funding from being used for the purchase or use of facial recognition technology, and for other purposes, H.R.3875, 116th Cong. (2019).

355. *See* H.R. 2231.

356. *See* S. 847.

Biometric Barriers Act would bar FRT use in public housing[357] and the FACE Protection Act would prohibit federal agencies from applying FRT to government-issued IDs without a court order.[358] Finally, H.R.3875 would prohibit using federal funds to purchase and utilize FRT.[359]

On the state level, California, Oregon, and New Hampshire have started to regulate FRT use in the public sector by banning the use of FRT in police body cameras.[360] Several states have also enacted laws to regulate FRT outside of law enforcement. Illinois passed the Biometric Information Privacy Act, which sets up significant restrictions on how private companies obtain and use an individual's biometric data.[361] This law requires firms that collect information to notify the person that his or her biometric profile is going to be collected, provide the reason for the collection, explain the length of time the information is to be collected, retained, and used, create a written, publicly available policy that details a retention schedule, and secure a written release from the person before collecting any biometric information or sharing the biometric data with another entity.[362] The Act also creates a private cause of action, allowing individuals to bring a suit for a mere violation of the law.[363]

New York enacted the Stop Hacks and Improve Electronic Data Security ("SHIELD") Act, which became effective on March 21, 2020.[364] The SHIELD Act requires businesses to implement protections for the "private information" of New York residents and expands the state's security breach notification requirements.[365] The SHIELD Act states that any business that stores the private information of New York residents, such as biometrics and driver's license information, must "develop, implement, and maintain reasonable safeguards to protect the security,

357. *See* H.R. 4008.

358. *See* H.R.4021.

359. *See* H.R.3875.

360. Benjamin Hodges & Kelly Mennemeier, *The Varying Laws Governing Facial Recognition Technology*, IP WATCHDOG (Jan. 28, 2020), https://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/. *See also* Assemb. Bill 1215, 2019-2020 Reg. Sess. (Ca. 2019). (California law prohibiting the use of FRT in body worn cameras until January 2023); H.R. 2571, 78th Or. Leg. Assemb., Reg. Sess. (Or. 2015).(Oregon law prohibiting the use of FRT to analyze body worn camera recordings); N.H. Rev. Stat. Ann. § 105-D:2 (2016). (New Hampshire law prohibiting the use of FRT to analyze body worn camera recordings).

361. Hodges & Mennemeier, *supra* note 361.

362. *Landmark Ruling on the Illinois Biometric Information Privacy Act*, WINSTON & STRAWN (Jan. 30, 2019), https://www.winston.com/en/thought-leadership/landmark-ruling-on-the-illinois-biometric-information-privacy-act.html.

363. *Id.*

364. Philip Gordon & Jennifer Taiwo, *The New York SHIELD Act: What Employers Need to Know*, SHRM (Aug. 28, 2019), https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/new-york-shield-act.aspx.

365. *ID.*

confidentiality, and integrity of the private information."[366] Unlike the law in Illinois, the SHIELD Act does not create a private cause of action. Instead, it enables the state's attorney general to enforce the mandates.[367]

Texas has a privacy act that forbids obtaining a person's biometric identifiers for commercial purposes unless the individual is first provided with notice and consents to the use. The state also limits the sale or disclosure of a person's biometric identifiers except under specific conditions.[368] Washington has a biometric protection law that bars any business or person from inputting biometric data into a database without giving notice, obtaining the person's consent, and offering a way to prevent subsequent use of the information for a commercial purpose.[369] Other similar state mandates include: 1) New Hampshire's statute prohibiting the Department of Motor Vehicles ("DMV") from using FRT when taking and retaining pictures,[370] 2) Maine's statute requiring state officials to issue rules that limit FRT use in drones,[371] 3) Washington's law requiring the DMV to notify license applicants that FRT may be used to verify their identities and restricting the disclosure of results[372] and 4) Missouri's statute prohibiting the Department of Revenue from using FRT to produce a license or identify licensees.[373]

The number of states regulating FRT is likely to grow since the legislatures of eleven other states have introduced bills limiting FRT-use in both the public and private sectors. These states are Idaho,[374] Indiana,[375] Maryland,[376] Massachusetts,[377] Michigan,[378] Minnesota,[379] Nebraska,[380] New Jersey,[381] South Carolina,[382] Vermont,[383] and

366. *Id.*

367. *Id.*

368. *State Biometric Privacy Legislation: What You Need to Know*, THOMPSON HINE(Sept. 5, 2019), https://www.thompsonhine.com/publications/state-biometric-privacy-legislation-what-you-need-to-know

369. *Id.*

370. N.H. REV. STAT. ANN. § 263:40-b (2014).

371. ME. REV. STAT. ANN. tt. 25, § 4501(5)(D) (2015).

372. WASH. REV. CODE ANN. § 46.20.037(3) (West 2012).

373. MO. REV. STAT. § 302.170 (2019).

374. H.R. 492, 65th Leg., 2d Reg. Sess. (Id. 2020).

375. H.R. 1238, 121st Gen. Assemb., 2d Reg. Sess. (In. 2020).

376. S. 613, Reg. Sess. (Md. 2019); *see also* S.46, Reg. Sess. (Md. 2020).

377. S.1385, 191st Gen. Court (Ma. 2019). ; S. 1429, 191st Gen. Court (Ma. 2019); H.R. 1538, 191st Gen. Court (Ma. 2019).

378. S. 342, 2019-2020 Leg. Sess. (Mich. 2019); H.R. House 4810, 2019-2020 Leg. Sess. (Mich. 2019).

379. S.1430, 91st Leg. (Minn. 2019); H.R. 1236, 91st Leg. (Minn. 2020).

380. S.746, 160th Leg., 2d Sess. (Neb. 2020).

381. S.116, 219th Leg., Reg. Sess. (N.J. 2020); G.A. 1210, 219th Leg., Reg. Sess. (N.J. 2020).

382. H.R. 4709, 123rd Sess. (S.C. 2020).

383. H.R. 470, 2019-2020 Reg. Sess. (Vt. 2019); H.R. 595, 2019-2020 Reg. Sess. (Vt. 2020).

Virginia.[384] Some cities have also started taking matters into their own hands. San Francisco, Oakland, and Somerville have passed ordinances that prohibit local authorities from using FRT.[385] In an unusual move, Portland, Oregon is taking steps to become the first city to ban both law enforcement and private entities from using FRT.[386] Finally, some law enforcement entities have voluntarily limited their use of FRT. For instance, the Seattle Police Department has stopped using FRT because of apprehension over bias and inaccurate results and the Detroit Police Department will only allow the utilization of FRT when it appears reasonably likely to help in the investigation of a violent crime.[387] The Utah Department of Public Safety has also placed restrictions on FRT in active criminal cases, and Portland, Oregon will likely soon follow suit.[388]

E. How Can the Defense Recognize a Facial Recognition Case

Facial identification obtained through a software application cannot be used in court as substantive evidence since the technology is not able to conclusively match a picture to an identity and there continue to be accuracy issues. Therefore, facial identification is not a scientifically reliable tool that can overcome a *Frye* or *Daubert* challenge.[389] At present, the technology should only be employed to develop leads in an investigation so its disclosure to defense counsel might not always be forthcoming.[390] As noted in *People v. Carrington*, "law enforcement [does] not use facial recognition technology as the sole basis to identify

384. H.R.J. Res. 59, 2020 Reg. Sess. (Va. 2020).

385. *See* S.F., Cal., Ordinance 107-19 (May 21, 2019) ("[I]t shall be unlawful for any Department to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained from Face Recognition Technology."); Ordinance Amending Oakland Municipal Code Chapter 9.64, ("[P]rohibit the City from acquiring, obtaining, retaining, requesting, or accessing Face Recognition Software."); Somerville, Mass., Ordinance 2019-16 (June 27, 2019) ("It shall be unlawful for Somerville or any Somerville official to obtain, retain, access, or use: (1) [a]ny face surveillance system; or (2) [a]ny information obtained from a face surveillance system.").

386. *See* Portland, Or., Ordinance (Nov. 08, 2019), *available at https://www.eff.org/files/2019/11/18/434828951-portland-unveils-facial-recognition-ban-proposal.pdf* ("Bureaus shall not acquire, evaluate or use Facial Recognition Technologies . . . [and] shall not use, access or retain any information derived from Facial Recognition Technologies"); *see also Developing a Facial Recognition Policy in Portland*, PORTLAND.GOV (Dec. 11, 2019), https://beta.portland.gov/bps/news/2019/12/11/developing-facial-recognition-policy-portland (explaining that a policy regulating FRT-use in the private sector is still at the research stage).

387. Hodges & Mennemeier, *supra* note 361.

388. Martin, *supra* note 299.

389. Kaitlin Jackson, *Challenging Facial Recognition Software in Criminal Cases*, NACDL (2019), https://www.nacdl.org/getattachment/548c697c-fd8e-4b8d-b4c3-2540336fad94/challenging-facial-recognition-software-in-criminal-court_july-2019.pdf; *see also* People v. Collins, 15 N.Y.S.3d 564,576 (Sup. Ct. 2015) (noting that the evidence that facial recognition technology produces has value, but it has not been accepted as reliable by relevant scientific communities).

390. Jackson, *supra* note 390, at 14.

or eliminate a suspect."[391] Therefore, the defense should learn how to recognize when FRT might have been used during a criminal investigation.[392] In this regard, the defense may present a viable challenge when facial recognition evidence is used to make an arrest without probable cause or in cases involving the arrest of the wrong person.[393]

Defense counsel should consider the possibility that the police used FRT to identify a suspect whenever there is a possibility of misidentification because the defendant was suspected of committing the offense from the initiation of the investigation, if there was a photo or video of the incident, or if there was an eyewitness to the event.[394] If the answer is yes to any of these questions, defense counsel should try to ascertain whether FRT was used.[395] This may involve a simple phone call to the prosecutor asking for clarification or the issuance of a discovery demand depending on the law in the jurisdiction.[396] This is important because the disclosure of facial recognition use may not be forthcoming since the government rarely intends to introduce the algorithm results at trial.[397]

Lynch v. State of Florida provides an example of where the defendant unsuccessfully tried to obtain the algorithm images. This matter involved the discovery of photographs generated by a facial recognition system of potential suspects other than the defendant.[398] The facts show that an undercover officer purchased crack cocaine from a person known as "Midnight."[399] During the purchase, an officer used his cell phone to take a picture of Midnight who was leaning into the car.[400] Subsequently, the officer sent the picture to a crime analyst who provided the police with the defendant's name and photograph as the result of database searches generated by the use of a facial recognition program.[401]

At trial, the defendant demanded that the government produce the other pictures in the databases of the people who were also known as "Midnight."[402] The court denied the request as being irrelevant and the defendant was found guilty. The defendant then asserted that the facial

391. People v. Carrington, No. B265888, 2018 WL 671903, at *11 (Cal. Ct. App. Feb. 2, 2018).
392. Jackson, *supra* note 390, at 15.
393. *Id.* at 16.
394. *Id.*
395. *Id.* at 16-17.
396. *Id.* at 17.
397. *Id.* at 20.
398. Lynch v. State, 260 So.3d 1166 (Fla. Dist. Ct. App. 2018).
399. *Id.* at 1168.
400. *Id.*
401. *Id.* at 1169.
402. *Id.*

recognition software had returned other pictures as possible matches. He contended that those pictures would have cast doubt on the state's case and that the government's failure to produce the images was a violation of *Brady v. Maryland*.[403]

The court rejected this argument because there was no reasonable probability that the trial results would have been any different if such a disclosure had been made.[404] The defendant could not show that the other pictures in the database resembled him to cause a misidentification nor could he show that anyone in those pictures would have been the culprit.[405]

F. Court Cases involving FRT

The government will rarely attempt to use the results of facial recognition software as the sole evidence in a criminal case. Rather, it is merely a tool that helps to develop other evidence and thus few criminal cases are devoted to the topic. Usually, discussions about facial recognition are in the context of a piece of evidence in the chain that led to the identification of a suspect. As noted in *People v. Carrington*, FRT is in its infancy and the science is evolving, as well as its reliability and accuracy.[406] At present, the government does not use FRT as "the sole basis to identify or eliminate a suspect."[407]

In a civil litigation context, FRT might arise in an invasion of privacy claim, or as a violation of a regulation of biometric technology against entities such as Shutterfly, Facebook, Microsoft, Google and other businesses that use FRT.

A Westlaw search using the words "facial recognition technology" disclosed 73 criminal and civil matters.[408] While the Fourth Amendment protects citizens against unreasonable searches, it is uncertain whether having images of the people's faces run through facial recognition systems constitutes a search. Like license plate readers, body-worn cameras and drones, FRT falls into a "constitutional grey area."[409] Existing case law, however, sheds some light on the possible outcomes once the issue inevitably reaches the Supreme Court. The next sections will provide examples of arguments that could be used in criminal cases to keep any reference about FRT out of evidence or permit its mention at

403. Brady v. Maryland, 373 U.S. 83 (1963).

404. Lynch, 260 So.3d at 1170.

405. *Id.*

406. *Carrington*, 2018 WL 671903, at *11.

407. *Id.*

408. This search was conducted by the authors on February 22, 2020.

409. Garvie et al., *supra* note 311.

the time of trial.

1. Cases That Would Support the Use of FRT in Court

U.S. v. Dionisio presents a Supreme Court analogy that would allow facial recognition technology to be a permissible police tool. This case dealt with a constitutional challenge to a grand jury subpoena requesting voice recordings from twenty individuals for identification purposes.[410] Dionisio and other witnesses refused to provide a voice recording and argued that being compelled to do so would violate their Fourth and Fifth Amendment rights.[411] The Supreme Court found that a person does not have a reasonable expectation of privacy over physical characteristics that he exposes to the public.[412] "No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."[413] The Court also opined that no valid Fifth Amendment claim had been raised since the privilege against self-incrimination prohibits compelling communications, not forcing a person to submit a photograph or to speak for identification purposes.[414]

Moreover, in *Smith v. Maryland*, the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[415] In *Smith*, the Government installed a pen register in the offices of a telephone company that was used to record the telephone numbers the defendant dialed.[416] Smith argued that he expected this information to remain private; but the Court disagreed.[417] The Court explained that when a person shares telephone numbers with a telephone company for business purposes, he cannot expect these numbers to remain a secret.[418] The judges essentially determined that a person assumes the risk "in revealing his affairs to another, that the information will be conveyed by that person to the Government."[419]

410. United States v. Dionisio, 410 U.S. 1, 3 (1973).

411. *Id.*

412. *Id.* at 14.

413. *Id.*

414. *Id.* at 6 (quoting Schmerber v. California, 384 U.S. 757 (1966)).

415. Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

416. *Id.* at 737.

417. *Id.* at 743-44.

418. *Id.* at 744.

419. *Id. But see* 18 U.S.C. § 3121(a) (overruling *Smith* by requiring a court order to install a pen register). "However, evidence obtained in violation of the statute can be admitted in criminal trials because violation of the statute does not result in an unconstitutional search and Congress did not provide for exclusion of evidence for violation of the statute." United States v. Allen, No. ACM 32727, 1999 WL 305093, at *6 (A.F. Crim. App. Apr. 22, 1999) (citing United States v. Thompson, 936, F.2d 1249 (11th Cir. 1991)).

Because the databases accessed by FRT are filled with photos voluntarily provided for licensing, employment, immigration, and other purposes, the third-party doctrine could be used to support the argument that the photos are not protected by the Fourth Amendment.

The Supreme Court eventually moved on from recognizing that certain information is not protected by the Fourth Amendment to determining that the use of certain technology to gather such information does not constitute a search. In *U.S. v Knotts*, the Supreme Court found that using warrantless monitoring of a beeper to track the defendant's movements did not violate the defendant's Fourth Amendment rights since there was no legitimate expectation of privacy.[420] The Supreme Court explained that the Fourth Amendment does not prohibit the police from "augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[421]

This decision suggests that FRT is merely another piece of permissible sensory-augmenting technology as it merely does something that the naked eye could do: look at two images and determine whether they portray the same person.

2. Cases That Would Oppose the Use of FRT in Court

The following are some of the cases suggesting that the use of FRT would violate the Constitution. Although a person does not have a reasonable expectation of privacy over his facial characteristics, some scholars rely on the two-prong test in *Katz v. Untied States* to argue that a person does have a reasonable expectation of privacy over his identity.[422] Under *Katz*, a violation of the Fourth Amendment only occurs when it can be shown that a subjective expectation of privacy is present, and that expectation is one that society acknowledges as being objectively reasonable.[423] The first prong of this test is satisfied because although people may expose their facial characteristics to the public, they often do not volunteer identifying information. The second prong is also fulfilled because the Supreme Court has made it clear that an expectation of privacy is reasonable if it is "established by general social norms."[424] Polls reveal that 60% of Americans feel that they should be able to be out in public without being identified and 93% believe that they should be able to control who obtains information about them, so it is not hard to

420. United States v. Knotts, 460 U.S. 276 (1983).

421. *Id.* at 282.

422. Katz v. United States, 389 U.S. 347, 360-61 (1967).

423. *Id.* at 361.

424. Robbins v. California, 453 U.S. 420, 428 (1981).

categorize privacy over our identity as a social norm.[425]

The capabilities of the technology itself and the fact that FRT is not in general circulation can be used to argue that the use of FRT constitutes a search. For instance, in *Kyllo v. United States*, the Supreme Court determined that law enforcement officials had performed an unlawful search when they relied upon thermal imaging technology not available for use by the general public to gather information about the inside of a house.[426] Similarly, FRT can only be used by law enforcement and large companies capable of compiling a database of pictures.[427] It could even be argued that FRT is used to view the bone structure underneath our skin "since that is what facial recognition software can essentially do: create a digital wireframe, or skeleton, of a person's face."[428]

While *Kyllo* addressed information-gathering technology that could have only been obtained through a physical intrusion, the Supreme Court has also addressed technology that gathers publicly available information. In *United States v. Jones*, Justice Alito suggested that a GPS device does more than augment the senses, since it allows law enforcement to do things that would otherwise be impracticable.[429] Although law enforcement could have followed the defendant, doing so for a month would have been costly, difficult, and impractical.[430] Similarly in *Carpenter v. United States*, the Court described the collection of cell-site location information as inescapable and automatic because, unlike a nosy neighbor, GPS devices "are ever alert, and their memory is nearly infallible."[431]

These cases suggest that the Court could find that FRT, unlike the beeper that signaled the presence of an automobile to a police receiver in *Knotts,* does more than augment "the sensory faculties bestowed upon them at birth."[432]

425. Mariko Hirose, *Privacy in Public Places: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1613 (2017).

426. Kyllo v. United States, 533 U.S. 27, 40 (2001).

427. With 350 million pictures being uploaded into Facebook and 95 million pictures being uploaded into Instagram every day, these platforms have access to over 290 billion pictures. Sean O' Hagan, *What Next for Photography in the Age of Instagram*, GUARDIAN (Oct. 14, 2018), https://www.theguardian.com/artanddesign/2018/oct/14/future-photography-in-the-age-of-instagram-essay-sean-o-hagan.

428. Elizabeth Snyder, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition Technology to Conduct Unlawful Searches*, 68 SYRACUSE L. REV. 255, 268 (2018).

429. Elizabeth E. John, *Artificial Intelligence and Policing: Hints in the Carpenter Decision*, 16 Ohio St. J. Crim. L. 281, 287 (2018).

430. *See* United States v. Jones, 565 U.S. 400, 429-30 (2012) (Alito, J., concurring) (explaining that this type of surveillance would have required several agents, multiple vehicles, and aerial assistance, which are resources that would have been reserved for cases of unusual importance).

431. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

432. United States v. Knotts, 460 U.S. 282-83 (1983).

3. First Amendment Concerns with FRT

There is also disagreement as to whether FRT may infringe on a person's First Amendment rights. In *Laird v. Tatum*, Vietnam War protestors argued that the government disregarded their First Amendment rights when Army surveillance tracked those who attended public meetings and kept a record of those who spoke.[433] The Supreme Court held that no valid claim had been presented since the government's surveillance did not have a deterrent effect.[434] The Court explained that the protestors' claim was based on the existence of the government's data-gathering system, and the Court refused to recognize that a deterrent effect could arise "merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that . . . the agency might in the future take some other and additional action detrimental to that individual."[435] *Laird*, therefore, suggests that using FRT to identify those in attendance at public events does not raise any First Amendment concerns.

However, some cases suggest that anonymity is a necessary safeguard to guarantee freedom of speech and association. For instance, in *NAACP v. Alabama*, the National Association for the Advancement of Colored People ("NAACP") refused to comply with a court order directing it to produce, among other things, a list of its members.[436] The Supreme Court recognized that there is a vital relationship between privacy and the freedom to associate, and therefore found that the court order would restrain the right of NAACP members to exercise such freedom.[437] The Court explained that complying with the court order could result in members withdrawing and dissuade others from joining out of fear that their beliefs would be exposed.[438]

Similarly, in *Talley v. California*, the Court found that an ordinance prohibiting the distribution of handbills unless they included the name and address of the person distributing them restricted freedom of expression.[439] The Court explained that persecuted groups have used anonymity to criticize oppressive practices and laws, and "identification and fear of reprisal might deter perfectly peaceful discussion of public matters of importance."[440]

Talley and *NAACP* provide the basis for arguing that FRT infringes on

433. Laird v. Tatum, 408 U.S. 1, 6 (1972).

434. *Id.* at 11.

435. *Id.*

436. NAACP v. Alabama, 357 U.S. 449, 451 (1958).

437. *Id.* at 462.

438. *Id.* at 463.

439. Talley v. California, 362 U.S. 60, 65 (1960).

440. *Id.* at 64-65.

a person's First Amendment rights. When FRT is combined with other forms of technology, it identifies individuals in attendance at protests, political rallies and religious ceremonies in real-time.[441] This would discourage attendance by those critical of the government and those who hold unpopular opinions out of fear that they will be identified and be subject to negative repercussions. After all, people tend to alter their behavior when they know or suspect that they are being watched.[442] Although FRT technology is being employed by law enforcement to carry out important responsibilities, it could come at the high cost of self-censorship.

4. Lower Court Cases Involving FRT

There are several lower court cases in which FRT played some role in the litigation. The earliest ruling allowing the use of facial recognition evidence occurred in San Francisco in 2011.[443] The case involved a defendant who had been convicted of murder and sentenced to twenty-five years in jail. The trial judge allowed the biometric proof to be admitted as evidence, which helped to exonerate the accused. The impact of FRT in this case surprised many legal professionals since the technology is still novel.[444]

Facial recognition software was used to help identify a criminal defendant when the video recording of an assault was posted on Facebook. In the case of *In re the Interest of K.M., A Minor,* the defendant contended that his conviction for aggravated assault and conspiracy was improper because he was only a bystander to the incident.[445] The evidence demonstrated that the victim was walking home from school when he was confronted by the defendant and his accomplices. The defendant filmed the encounter between the victim and his co-conspirators in which the student was punched and kicked for no reason.[446] The video was then posted on YouTube and the police identified the defendant through facial recognition software on Facebook. The suspect was arrested and his

441. In 2016, nine out of thirty-eight body-worn-camera manufacturers had incorporated facial recognition technology into their units or were contemplating it. Katelyn Ringrose, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57, 60 (2019).

442. *See Americans' Privacy Strategies Post-Snowden*, PEW RES. CENTER 4 (Mar. 16, 2015), https://perma.cc/D54F-G343 (noting that after learning about NSA surveillance from Edward Snowden's revelation, 22% of America adults changed their online behavior).

443. *A First: Biometrics Used to Sentence Criminal*, HOMELAND SECURITY NEWS WIRE (Feb. 1, 2011), http://www.homelandsecuritynewswire.com/first-biometrics-used-sentence-criminal.

444. *Id.*

445. *In re* K.M., No. 2721 EDA 2014, 2015 WL 7354644 (Pa. Super. Ct. Nov. 20, 2015).

446. *Id.*

phone, which was seized under a warrant, contained the video of the fight.[447] The court upheld the identification and properly adjudged the juvenile delinquent since his phone's camera was running before the assault. The running camera suggested that the attack was planned and that the parties were working together moments before the assault, thereby creating the inference that they agreed that one or more of them would participate in the confrontation.[448]

Geiger v. Maryland involved theft by deception.[449] The facts show that a tire store employee received a call from a Brian Johnson requesting tires for his car. The next day, Johnson went to the store and orally provided his credit card number, since he claimed that he did not have the card with him.[450] As an additional measure of identification, he produced a North Carolina driver's license that contained his picture. It turned out that the credit card was stolen, and the driver's license was fake.[451] Johnson's picture from the license was run through a database and facial recognition software matched it to a Maryland driver's license. The judge was shown both pictures at trial, and the court determined that they showed the same man.[452]

During the testimony of the investigating detective, the state offered into evidence a copy of the Maryland picture that was located though FRT. The defense vigorously protested the picture's introduction but the trial judge ruled that the defendant "doesn't have a right to protect his image," and it was defense counsel who mentioned facial recognition technology in the first place.[453] The court opined that no error had been committed because the computerized identification was not being used as evidence but was simply a guide used by the detective to put the investigation "on the right track."[454] At no time did the detective testify in any manner about FRT and the state never questioned him about facial profiling.[455] Therefore, when utilized to direct the investigation, the use of FRT technology did not invalidate the defendant's conviction.[456]

In *United States v. Gibson*, the defendant secured a Florida driver's license under the false name of Gregory Gibson.[457] He then applied for a

447. *Id.*
448. *Id.* at 6.
449. Geiger v. Maryland, 174 A.3d 954, 956 (Md. 2017).
450. *Id.* at 956.
451. *Id.* at 957.
452. *Id.*
453. *Id.* at 964.
454. *Id.* at 965.
455. *Id.*
456. *Id.*
457. United States v. Gibson, No. 8:00-CR-442-T-27AEP, 2016 WL 845272, at *2 (M.D. Fla. Mar. 4, 2016).

passport and submitted a false application under the fictitious name. The application was flagged as fraudulent and the authorities tried to locate the defendant to no avail.[458] Several years later, an analyst conducted a facial recognition check and linked the fake picture to the driver's license of Anthony Lazzara. This individual was arrested at the address listed on the valid license.[459] A subsequent fingerprint search revealed a host of aliases and a criminal record linked to the defendant.[460]

The defendant objected to the time delay between when he submitted the false passport application and his trial.[461] His motion to dismiss the case as a violation of the right to a speedy trial, however, was denied. The court noted that the defendant caused the delay by using various aliases and false identifications.[462] This deception thwarted his apprehension through traditional investigative tools such as the fingerprint database. The agent further stated that he did not have initial access to FRT because of privacy concerns.[463] Therefore, any delay on the part of the government was considered a slight negligence at the worst and the defendant did not suffer any prejudice.[464]

Montanez v. Department of Transportation involves a suspension of a driver's license in Pennsylvania. In *Montanez*, facial recognition software determined that the defendant had obtained a driver's license using a false identity.[465] The driver had received multiple citations over a period of time from 2006 to 2010 under the name of DeLeon. He used the name Montanez to obtain a different license in 2013 as well as a commercial driver's license in 2016. In 2017, Montanez renewed his driver's license and the Department of Transportation used facial recognition software to compare driver's license pictures to others in the government's database.[466] At this time, the Department of Transportation learned that DeLeon and Montanez were the same person. While the court never discussed the use of FRT, it upheld the suspension of the license because of the fraud perpetrated by the defendant—which necessarily rested on the use of FRT.[467]

In the case of *In re Matter of the Search of a Residence in Oakland*, two individuals were suspected of engaging in extortion via Facebook

458. *Id.* at *2.
459. *Id.*
460. *Id.*
461. *Id.* at *1.
462. *Id.* at *2.
463. *Id.* at *3.
464. *Id.*.
465. Montanez v. Dep't of Transp., No. 1150 C.D. 2018, 2019 WL 2997381, at *2 (Pa. Commw. Ct. 2019).
466. *Id.*
467. *Id.* at *4-5.

Messenger.[468] The Government sought to seize the electronic devices located at the suspects' residence, and the court found that the facts in the affidavit supported a finding of probable cause.[469] However, the Government also sought to compel any individuals located at the residence to use their biometric features (such as a fingerprint or a facial scan) to unlock the electronic devices to search their contents.[470] The Court found that this subsequent request violated the Fifth Amendment privilege against self-incrimination.[471]

The Court reached this conclusion by first noting that courts have previously held that suspects cannot be compelled to provide the passcode for an electronic device.[472] The Court recognized that while some acts could qualify as testimonial "if conceding the existence, possession, and control, and authenticity of the documents tended to incriminate them," other acts such as providing a blood sample or a fingerprint did not constitute a communication.[473] The Court finally concluded that compelling the use of biometric features to unlock a device was not akin to compelling someone to submit to fingerprinting or provide a DNA sample for two reasons.[474] First, biometric features in these types of cases serve the same purpose as a passcode, so if a person cannot be compelled to provide his or her passcode the person cannot be compelled to use their biometric features.[475] Second, while compelling someone to submit to fingerprinting merely confirms whether he or she is the source of physical evidence,[476] compelling someone to use biometric features to unlock a device confirms ownership or control of the device as well as control or significant connection to its contents.[477]

FRT has also been addressed in civil suits against private entities. In *Monroy v. Shutterfly, Inc*, several individuals sued Shutterfly for collecting and using their facial geometry without their consent in

468. *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019).

469. *Id.*

470. *Id.*

471. *See id.* at 1013-14 (explaining that the court also found that the Government's request violated the Fourth Amendment because it was not limited to a particular person or device and the Government could not be allowed to search a non-suspect's device simply because they are present during a lawful search).

472. *Id.* at 1015 ("The expression of the content of an individual's mind falls squarely within the protection of the Fifth Amendment.").

473. *Id.*

474. *Id.*

475. *Id.* at 1015-16.

476. *Id*. at 1016.

477. *See id.* ("With a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.").

violation of Illinois' Biometric Information Privacy Act ("BIPA").[478] Shutterfly moved to dismiss the complaint by claiming that BIPA did not cover facial geometry obtained from photos and that plaintiffs failed to allege actual damages.[479] Guided by the statutory definitions, the court concluded that a facial scan did not constitute "biometric information,"[480] but did constitute a "biometric identifier."[481] The court explained that a facial scan was referenced in the definition of "biometric identifier,"[482] and limiting these scans to those obtained in person was not supported by the statute's purpose of "protecting privacy in the face of emerging biometric technology."[483] As for Shutterfly's second claim, the court found that BIPA does not require a showing of actual damages to state a claim.[484] The court reached this conclusion by noting that other statutes have been interpreted to allow recovery without a showing of actual damages.[485]

In *Patel v. Facebook, Inc*. several website users filed suit against Facebook, claiming that the social media giant used facial-recognition technology without complying with BIPA.[486] The case involves Facebook's feature known as "Tag Suggestions". If activated, Facebook may use FRT to ascertain whether the customer's friends are contained in pictures uploaded by that user. If a picture is downloaded, FRT will scan the image to see if it includes any faces of known people.[487] If known people are present in the image, the software detects the geometric data points that generate a face signature or a map. The software then compares the face signature to other images in the company's database of user face templates. If a match is found, Facebook informs the user to tag the person in the picture.[488]

Facebook filed a motion to dismiss the complaint for lack of standing because the plaintiffs had not claimed any identifiable injury. This motion was denied and an appeal was taken of that determination.[489] In upholding this decision, and certifying the matter as a class action, the 9th Circuit found that "an invasion of an individual's biometric privacy rights has a

478. Monroy v. Shutterfly, Inc., No. 16 C 10984, 2017 U.S. Dist. LEXIS 149604, at *2-3 (N.D. Ill. Sept. 15, 2017).
479. *Id.* at *5.
480. *Id.* at *7.
481. *Id.* at *14.
482. *Id.* at *8.
483. *Id.* at *14.
484. *Id.* at *26.
485. *Id.* at *23-25.
486. Patel v. Facebook, Inc., 932 F.3d 126, 1267 (9th Cir. 2019).
487. *Id.* at 1268.
488. *Id.*
489. *Id.* at 1269-70.

close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[490] Once Facebook creates a face template of that person, the potential uses are endless. The company can use the information to tag the user in the hundreds of millions of photos uploaded to Facebook each day and identify whether the person's Facebook friends are also present in the picture.[491] According to the court, Facebook's assemblage, use, and storage of customer's facial templates is the very harm contemplated by the statute.[492] Facebook appealed this adverse ruling to the Supreme Court, but the Court denied certiorari .[493]

On January 30, 2020, Facebook settled this claim for $550 million, marking one of the largest settlements ever made in a privacy lawsuit.[494] Paul Geller--one of the attorneys representing the plaintiffs-- admitted he was "hopeful that this case is a turning point for privacy litigation. Technology is advancing at a rapid pace, and corporations need to realize that they better tread carefully when it comes to recognizing, tracking and monitoring us."[495]

Google is currently facing a similar lawsuit in the U.S. District Court for the Northern District of California. The complaint alleges that Google violated BIPA by collecting biometric identifiers through its photo-sharing cloud service without written consent from users.[496] Specifically, the complaint states that Google used FRT to create face templates and that "each face template that Google extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person."[497] The suit seeks $5,000 for each BIPA violation and an injunction to stop Google from continuing this practice.[498]

490. *Id.* at 1273.

491. *Id.*

492. *Id.* at 1275.

493. Nathan Freed Wessler, *A Federal Court Sounds the Alarm of the Privacy Harms of Face Recognition Technology*, ACLU (Aug. 9, 2019), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/federal-court-sounds-alarm-privacy-harms-face.

494. Thomas Germain, *Facebook Settles $550 Million Facial Recognition Lawsuit*, CONSUMER REP. (Jan. 30, 2020), https://www.consumerreports.org/lawsuits-settlements/facebook-settles-facial-recognition-lawsuit/.

495. *Id.* at *3.

496. Ross Todd, *Google Hit with Class Action under Illinois Biometric Privacy Law over Facial Recognition*, LAW.COM (Feb. 7, 2020), https://www.law.com/therecorder/2020/02/07/google-hit-with-class-action-under-illinois-biometric-privacy-law-over-facial-recognition/.

497. Lauren Berg, *Google Accused of Collecting User 'Face Prints' from Photos*, LAW360 (Feb. 7, 2020, 5:14PM), https://www.law360.com/articles/1241866/google-accused-of-collecting-user-face-prints-from-photos.

498. *Id.*

5. Court Cases involving FRT in Other Countries

The struggle over the use of FRT is not limited to the United States. A British court recently found that the use of FRT by police is lawful, thwarting the efforts to limit FRT by an activist concerned about the tool's implications for privacy.[499] The opinion was decided while a worldwide debate concerning the growing use of FRT was taking place.[500] Advances in artificial intelligence have made it simpler for law enforcement to automatically scan faces and promptly match those images to "watch lists" of suspects, missing people and those of interest, but the technology also presents apprehension about mass surveillance.[501]

The Plaintiff in the British case claimed that the police scanned his face twice as it assessed the technology. The first instance occurred while he was Christmas shopping and the second when he was at a protest.[502] The plaintiff asserted that "[t]his sinister technology undermines our privacy and I will continue to fight against its unlawful use to ensure our rights are protected and we are free from disproportionate government surveillance."[503] The court disagreed, stating that the use of facial recognition technology by the police was consistent with British human rights and data privacy laws because the images and biometric data of those who were not a match on the "watch list" were promptly deleted.[504] The court did note, however, that its legal analysis should be periodically reviewed.[505]

In Canada, the Ontario Court of Justice considered a case involving facial recognition technology in *R. v. Voong*.[506] The defendant was arrested after FRT identified him as having seven fraudulent driver's licenses in the Ministry of Transport database.[507] In the past, three of these license cardholders had failed to appear in court for traffic violations so the Crown had charged Mr. Voong for possession of fraudulent driver's license possession under the Canadian Highway Traffic Act.[508] The defendant asserted that the evidence was obtained through an

499. Kelvin Chan, *Activist Loses UK Court Case on Police Fascial Recognition*, ASSOCIATED PRESS (Sept. 4, 2019), https://abcnews.go.com/Technology/wireStory/activist-loses-uk-court-case-police-facial-recognition-65378750.

500. *Id.*

501. *Id.*

502. *Id.*

503. *Id.*

504. *Id.*

505. *Id.*

506. R. v. Voong, 2018 ONCJ 352 (Can.).

507. Ali Imrie, *Ontario Court of Justice: Facial Recognition Technology of Driver's License Photos Not a Privacy Violation*, RIGHTS WATCH BLOG, CANADIAN CIVIL LIBERTIES ASS'N (Feb. 6, 2018), http://rightswatch.ca/2018/06/02/18391/.

508. *Id.*

unreasonable search according to the Canadian Charter of Rights and Freedoms.[509]

The Ontario Court of Justice disagreed and noted that the Charter did not apply to pictures and materials provided with the driver's license application since there were no relevant privacy considerations.[510] The Ministry of Transport has the authority to disclose information in its files to other agencies. Therefore, the defendant has no reasonable expectation of privacy and his rights were not violated.[511]

One Russian court has rejected a claim to ban FRT.[512] A woman, Alena Popova, was involved in a sexual harassment protest in Moscow in 2018. Subsequently, she was fined for protesting after being identified through FRT.[513] This government action prompted her to sue the Moscow police claiming that they were "indiscriminately" collecting biometric information through facial recognition software without consent.[514] The court dismissed the claim. The police maintained that Popova had no proof that FRT was used to identify her.[515] It should be noted that this case comes at a time that Moscow is planning to expand its use of FRT as its mounts 160,000 cameras around the city, making it one of the largest users of FRT in the world.[516] This move has prompted objections by several organizations. For instance, Amnesty International has criticized the plan to expand the utilization of facial-recognition systems, saying their anticipated use in Moscow during public assemblies will "inevitably have a chilling effect" on protesters.[517]

Chinese courts were asked to address FRT use for the first time just last year. A Chinese law professor sued a wildlife park after being required to scan his face to enter the park.[518] The law professor was an annual pass-holder who learned that the park had replaced its fingerprint identification system with a facial recognition system.[519] Annual pass-holders who

509. *Id.*

510. *Id.*

511. *Id.*

512. Emily Sherwin & Elena Barysheva, *Russian Court Rejects Call to Ban Facial Recognition Technology*, DW(June 1, 2019), https://www.dw.com/en/russian-court-rejects-call-to-ban-facial-recognition-technology/a-51135814.

513. *Id.*

514. *Id.*

515. *Id.*

516. *Id.*

517. *Watchdog Warns About 'Chilling Effect' of Russia's Use of Facial-Recognition Technology*, RADIO FREE EUROPE RADIO LIBERTY (Jan. 31, 2020), https://www.rferl.org/a/watchdog-warns-about-chilling-effect-of-russia-s-use-of-facial-recognition-technology/30410014.html.

518. Shan Li, *Chinese Professor Files Rare Lawsuit Over Use of Facial-Recognition Technology*, WALL ST. J. (Nov. 4, 2019, 12:27 PM), https://www.wsj.com/articles/chinese-professor-files-rare-lawsuit-over-use-of-facial-recognition-technology-11572884626.

519. *Id.*

refused to undergo a facial scan were not allowed into the park and were not reimbursed for the value of their membership.[520] According to the lawsuit, this violated China's consumer protection law since it forced customers to provide biometric information without their consent.[521] Although the law professor is seeking a refund for his membership, he claims to have filed the lawsuit primarily to "raise awareness about the problems that come from the unregulated collection of personal data and to call for increased regulation and compliance."[522]

China does not have laws regulating the collection, storage, and use of information gathered through FRT despite being one of the biggest users of this technology.[523] The Chinese government is known to support companies that develop FRT to bolster commerce and ensure public safety.[524] FRT is widely used in Chinese airports, railway stations, offices, campuses and residential buildings.[525] China also uses the technology to arrest jaywalkers and those who commit other summary offenses.[526] Although there was a "public willingness to surrender some privacy in exchange for the safety and convenience," concerns have risen after it was reported that facial data was being sold online for as little as $1.40.[527] A new law requiring phone service providers to scan the faces of new customers has also led some to speculate that the government is using FRT to keep track of its population.[528] Many are now calling for a ban on FRT use, and the outcome of this lawsuit could lead the government to devise laws that regulate how private companies and law enforcement use the technology.[529]

V. CONCLUSION

This article aims to show the extent to which law enforcement relies upon recent developments in camera surveillance, automated license plate readers, drones, and facial recognition systems to carry out its duties.

520. *Id.*

521. *Id.*

522. *Id.*

523. *China Facial Recognition Case Puts Big Brother on Trial*, HONG KING FREE PRESS (Jan 12, 2020), https://www.hongkongfp.com/2020/01/12/china-facial-recognition-case-puts-big-brother-trial/.

524. *Id.*

525. *A Lawsuit Against face-scan in China Could Have Big Consequences*, ECONOMIST (Nov. 9, 2019), https://www.economist.com/china/2019/11/09/a-lawsuit-against-face-scans-in-china-could-have-big-consequences.

526. Martin, *supra* note 299.

527. *China Facial Recognition Case Puts Big Brother on Trial*, *supra* note 524.

528. Sam Shead, *Chinese Residents Worry About the Rise of Facial Recognition*, BBC (Dec. 5, 2019), https://www.bbc.com/news/technology-50674909.

529. Li, *supra* note 519.

Unfortunately, laws regulating these various forms of technology have not been able to keep pace with developments, and law enforcement has been able to utilize digital advances with few restrictions. Although this technology offers a vast array of benefits, it is important to be mindful that these digital developments may infringe on the Constitutional rights of citizens. Some state legislatures and lower courts have taken steps to safeguard or minimize this intrusion, but the degree to which the civil liberties of citizens are protected should not depend upon the state in which they live. Rather than waiting for the Supreme Court to resolve the various constitutional issues raised by this new technology, Congress should enact legislation that ensures the use of these digital advancements is limited, transparent, and accurate. These systems are only going to become more sophisticated over time and the government will be able to monitor the minute-by-minute movements of its citizens with relative ease. Therefore, safeguards need to be implemented so that members of society do not feel like Big Brother is watching at every corner and turn.