NOTES

ORWELL'S *1984* "BIG BROTHER" CONCEPT AND THE GOVERNMENTAL USE OF FACIAL RECOGNITION TECHNOLOGY: A CALL TO ACTION FOR REGULATION TO PROTECT PRIVACY RIGHTS

TATE DUCKER*

* Juris Doctor candidate, Belmont University College of Law, 2021; B.S., North Carolina State University, 2018. I want to thank Ben Powers for providing initial guidance and direction with this note's topic. Additional thanks to Professor Jeffrey Usman for his support and assistance throughout the note writing process. Finally, I would like to thank all editors of the *Belmont Law Review* for their diligent work in editing this note.

INTRODUCTION

George Orwell once wrote in his novel, *1984*, that "[i]t was terribly dangerous to let your thoughts wander when you were in any public place or within a range of a telescreen. The small things could give you away. A nervous tic, an unconscious look of anxiety, a habit of muttering to yourself – anything that carried with it the suggestion of abnormality, of having something to hide. In any case, to wear an improper expression on your face [] was a punishable offense."[1] The *1984* novel was written in the year 1949, a time long before the advancement of the current technology in use today,[2] yet Orwell was fearful, as his writing demonstrated, of what the future could hold—of the potential for modern societies to implement technology with enormous investigative and authoritative capabilities.[3] The *1984* novel displayed themes of totalitarianism and of a dystopian future, where an all-seeing leader known as "Big Brother" becomes a universal symbol for intrusive and oppressive government oversight.[4] Orwell was not necessarily a prophet, but instead a writer, who recognized that a government's power to control an individuals' actions and thoughts could be drastic for society.[5]

Fast forward to the present day. The year is 2020. Technology has expanded at an explosive rate and has revolutionized the world we live in today.[6] Modern technology continues to pave the way for providing substantial tools and resources at our fingertips. Consider how far society has come in the past fifty years. What was once only a dream of technological capabilities, portrayed only in science fiction novels, has now

1. GEORGE ORWELL, 1984 65 (1949).

2. *George Orwell's "1984" is Published*, HISTORY (Nov. 13, 2009), https://www.history.com/this-day-in-history/george-orwells-nineteen-eighty-four-is-published [https://perma.cc/P5U8-JW74].

3. *See* ORWELL, *supra* note 1.

4. *See George Orwell's "1984" is Published*, *supra* note 2.

5. Matthew Feeney, *Seventy Years Later, It's Still '1984'*, CATO INST. (June 5, 2019), https://www.cato.org/publications/commentary/seventy-years-later-its-still-1984?gclid=CjwKCAiAjrXxBRAPEiwAiM3DQjzWCMm-bo2f4sDf_MKkrVYbGqfQL9tIuHRES1nx1KvA3npjx5jzjBoCT-gQAvD_BwE [https://perma.cc/64B4-EHSY].

6. Leslie Wilder, *7 Ways Technology Has Changed Our Lives*, THRIVE GLOB. (May 29, 2019), https://thriveglobal.com/stories/7-ways-technology-has-changed-our-lives/ [https://perma.cc/5Q38-ZYML].

come to life.[7] Developments in technology have led to improved communication, better home entertainment, improved housing and lifestyle, and convenience with daily tasks.[8] Yet, like anything else, with the good comes the bad. Business Insider noted how, from a consumer standpoint, the use of technology has been detrimental to physical health, mental health, relationships, and the ability to interact face to face with other people.[9]

Likewise, the increase of technology has largely changed the nature of the relationship between the government and its citizens as it relates to surveillance of movements throughout daily life. Today, 600 separate United States government agencies employ the use of facial recognition technology.[10] This technology uses cameras to capture images of the person and her biometric identifying data.[11] The captured biometric data is then converted into a template, which is then compared to preexisting images of the person to determine her identity.[12] The use of facial recognition technology has begun to fuel debates over its *unregulated* use which has been termed a "massive breach of privacy and trust."[13] Others defend the use of facial recognition technology as an important tool for stopping crime.[14] To be sure, the lack of regulation in the government's use of facial recognition technology raises questions and concerns. Is this technology the "Big Brother" that Orwell's *1984* novel warned us against? Do individuals

---

7. Janna Anderson & Lee Rainie, *Concerns About the Future of People's Well Being*, PEW RES. CTR. (Apr. 17, 2018), https://www.pewresearch.org/internet/2018/04/17/concerns-about-the-future-of-peoples-well-being/ [https://perma.cc/CGX9-MWWB].

8. Zlatko Stojanov, *The 6 Main Ways Technology Impacts Your Daily Life*, TECH.CO (Feb. 23, 2017, 8:30 PM), https://tech.co/news/6-main-ways-technology-impacts-daily-life-2017-02 [https://perma.cc/7PYL-S37U].

9. Chelsea Greenwood, *9 Subtle Ways Technology is Making Humanity Worse*, BUS. INSIDER (Aug. 23, 2019, 10:20 PM), https://www.businessinsider.com/technology-negative-bad-effects-society-2019-8 [https://perma.cc/CQB8-HV9M].

10. Editorial Board, *A Scary New Facial Recognition Tool Underlines the Urgent Need for Privacy Laws*, WASH. POST (Jan. 23, 2020, 3:48 PM), https://www.washingtonpost.com/opinions/a-scary-new-facial-recognition-tool-underlines-the-urgent-need-for-privacy-laws/2020/01/23/6c2646a8-3d37-11ea-baca-eb7ace0a3455_story.html [https://perma.cc/PY2G-X6SP].

11. 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 Jan. 26, 2020) [https://perma.cc/G39V-LGBY].

12. *Id.*

13. Drew Harwell, *Facial-Recognition Use by Federal Agencies Draws Lawmakers' Anger*, WASH. POST (July 9, 2019, 5:19 PM), https://www.washingtonpost.com/technology/2019/07/09/facial-recognition-use-by-federal-agencies-draws-lawmakers-anger/ [https://perma.cc/G8R4-SE72].

14. *Id.*

have privacy rights and expectations against the use of this technology? If so, what are the appropriate regulatory measures for protecting privacy rights?

This note serves as a call to action imploring legislatures, specifically the United States Congress, to adopt comprehensive statutory regulation to regulate the governmental use of facial recognition technology and the compilation of biometric data. This note will proceed in five parts. Following this Section, Section I dives into an overview and discussion on the details of facial recognition technology, including a summary of biometric data and the current uses of facial recognition technology in the United States. Section II discusses key aspects of current state laws that regulate facial recognition technology. Section II transitions into exploring current proposed federal law that will regulate the commercial use—not governmental use—of facial recognition technology. Section III reviews Fourth Amendment law and constitutional requirements. Section IV applies these Fourth Amendment principles to the issue of a government's unregulated use of facial recognition technology. Section V proposes legislation to further protect American citizens' privacy rights. Secondary to the proposed legislation, Section V will further examine policy considerations and arguments for extending protection.

I. BACKGROUND ON FACIAL RECOGNITION TECHNOLOGY, DATA COLLECTION, AND CURRENT USES OF FACIAL RECOGNITION TECHNOLOGY

A. What is Facial Recognition Technology?

Facial recognition technology is a method for identifying and verifying the identity of an individual using their face and its distinguishing features.[15] This technology falls under the grander purview of biometric technologies, which involves a five-part process.[16] First, a sensor collects information on a particular characteristic of an individual and then converts that information into a digital format.[17] From there, signal processing algorithms convert the digital format to a digital biometric template.[18] These computer algorithms, within the software applications, can measure specific details such as the distance between the eyes, the width of the nose, or the length of the jawline.[19] Once the new template is produced, it is

15. *Face Recognition*, ELEC. FRONTIER FOUND. (Oct. 24, 2017), https://www.eff.org/pages/face-recognition [https://perma.cc/P5DL-97DW].

16. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:4 *Biometrics: A General Overview of Biometric Technology*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).

17. *Id.*

18. *Id.*

19. *See* Hamann & Smith, *supra* note 11.

stored in a data storage system to allow for later comparison against new biometric templates that are generated in the future.[20] At a later time, either the same sensor or a separate sensor will collect the same individual's biometric identifying information, using the same particular biometric authentication system, which then forms a new template and compares the new template to existing templates by using a matching algorithm.[21] The results from the matching algorithm are then used to decide the identity of the individual.[22]

This five-step identifying process serves two distinct objectives: namely, (1) ascertaining whether the individual is whom she purports to be, or (2) attempting to determine the individual's identity.[23] In other words, the first function of facial recognition technology seeks to verify the identity of an individual by asking the question of: Are you whom you claim you are?[24] The first function commonly involves one-to-one matching,[25] which scans an individual's biometric trait that is then compared to existing templates on that individual.[26] Verification often proves to be an easy process because these persons have already provided their biometric identifying information once. Thus, all that is sought is to determine whether the person is who they say they are.[27] For example, facial recognition technology software often takes photos from social media sites or other online websites, where social media users willingly submit photos of their faces.[28] One common example of current uses is Facebook, where users submit photos and then, using Facebook facial recognition technology, tag their suggested friends in the photo.[29]

Second, facial recognition technology seeks to determine the identity of an individual by asking the question of: Who are you?[30] This function is a much more complex process than the first function. Like the first function, the second function involves one-to-one matching, but identification compares the newly created biometric trait with an entire database.[31] The goal with identification is to find a matching template, if

20. FISHMAN & MCKENNA, *supra* note 16.
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*; CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:45 *Biometrics and Social Media*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).
30. FISHMAN & MCKENNA, *supra* note 16.
31. *Id.*

one exists, to determine the identity of the individual.[32] A more detailed analysis regarding biometric data collection is discussed next.

B. Facial Recognition Technology and Collection of Biometric Data

Touched on above, facial recognition technology systems collect distinct facial characteristics, known as *biometrics*,[33] that are then compared to pre-existing biometric templates using facial recognition software applications.[34] The term biometrics can be used interchangeably to describe a (1) characteristic or a (2) process.[35] Biometrics as a *characteristic* are "measurable biological (anatomical and physiological) and behavioral characteristics capable of being used for automated recognition."[36] Biometric data as *characteristics* roughly fall into two categories: (1) physical identifiers and (2) human identifiers. Typical physical identifiers include fingerprint recognition, hand geometry, retina scans, iris scans, voice recognition, face recognition, and vascular or vein recognition. It is estimated that at least 14% of private companies currently use such technology to obtain biometric identifying information.[37]

Biometrics can also be described as a *process* that employs "automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics."[38] More recently, the focus of biometric identifying technology and its uses has focused on collecting information on behavioral identifiers.[39] Where this technology once only had the capability of capturing one's physical identifying qualities, it has now grown to capabilities of allowing users to gain valuable information on a person's typing patterns, physical movement patterns, navigation patterns, and engagement of technology patterns.[40]

---

32. *Id.*

33. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:1 *Biometrics: Introduction*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).

34. *Id.*

35. *Id.*

36. *Id.*

37. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:44 *Biometrics: Private Industry Use*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).

38. FISHMAN & MCKENNA, *supra* note 33.

39. *Id.*

40. *Id.*

C. History of Biometric Data Collection and Use of Facial Recognition Technology

Although facial recognition technology is a relatively new phenomenon, the use of biometric data, and its form of identification, has been around for centuries.[41] The federal government first began to obtain biometric data in 1907 when the Department of Justice established a Bureau of Criminal Identification based on fingerprint data.[42] By the 1960's, the federal government's use of compiling biometric data had become a big emphasis with federal protection agencies. Specifically, the Federal Bureau of Investigation began to create an automated technology system for a database of fingerprints with the ability of comparison.[43]

Around this same time, private industries, like government agencies, began to invest heavily in developing new biometric identification technologies.[44] By the early 1990s, facial recognition software began to increasingly develop, and by 1993, the Department of Defense initiated its Face Recognition Technology program.[45] By as early as 1996, the United States Army implemented real-time face identification.[46]

Early 21st century uses of facial recognition technology remained primarily in the national defense sphere.[47] In 2000, the Defense Advanced Research Projects Agency (DARPA) created the Human Identification at a Distance Program,[48] which sought to create an algorithm to identify individuals from up to 150 meters away by using face and gait (a person's manner of walking) technologies.[49] The push for the development of facial recognition technology software greatly increased after the 9/11 terrorist attack.[50] Post-9/11 efforts would act as a strong impetus in developing and implementing new biometric identification systems to collect, retain, and share individual biometric data.[51]

The first reported use of wide-scale biometric collection through facial recognition technology occurred at the 2001 Super Bowl in Tampa, Florida.[52] As excited fans passed through the gates outside the stadium,

---

41. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:2 *Biometrics: A History*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).
42. *Id.*
43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*

video surveillance captured images of attendees and sent them to a computer.[53] Once the computer received these images, the images would then be matched to law enforcement's existing agency biometric data files.[54] Unknown to the public at this time is that for many years, biometric technology had been in use throughout the law enforcement sector, including aiding border control efforts, overseeing driver's license applications and the photos taken, for security clearance purposes, and preventing welfare fraud.[55] Privacy law scholars Fishman and McKenna would ultimately call the evolution of biometric identifying information and its use in stopping crime "remarkable."[56]

Since the inception of facial recognition technology, its uses and success have recognized significant advances.[57] This has largely come due to social media sites use of facial recognition technology, the growth of smartphone applications, the successful implementation of facial recognition in airports, and nationally centralized collection of facial biometric data in criminal and military investigations.[58] Moreover, in a commercial setting, these low-cost facial recognition technologies are being developed and put into use at an astounding pace.[59] As of current, consumer-grade cameras with built-in face detection are readily available for sale to consumers.[60] These advances and improvements are backed by statistics as well.[61] The technology error rate has recognized 50% drops in error every two years.[62] What history shows is that the types of biometric technology in use is greatly expanding at a rapid rate. Discussed below is the current state of the law with regard to regulation of facial recognition technology.

53. *Id.*
54. *Id.*
55. *Id.*
56. *Id.*
57. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:11 *Biometrics Identification: Facial or Face Recognition*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).
58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.*

II. CURRENT FEDERAL AND STATE REGULATION OF FACIAL RECOGNITION TECHNOLOGY

States have led the way in regulating the collection and compilation of biometric data.[63] However, the current state laws that do exist regulate the commercial[64]—not governmental[65]—use of facial recognition technology and collection of biometric identifying information.[66] Illinois was the first state to adopt a comprehensive act that would regulate the commercial use of facial recognition technology.[67] Texas and Washington soon thereafter followed Illinois' footsteps in developing comprehensive "biometric" legislation.[68] Other states have begun to follow suit in proposing legislation to address the use and collection of biometric data.[69] The discussion below will touch on the Illinois statute and its key provisions. Following thereafter will be a brief overview of other comprehensive state laws enacted by Texas and Washington with their distinguishing characteristics.

With respect to federal law, there is currently no regulation of commercial use of facial recognition technology nor governmental use of technology. The current federal comprehensive act that has been proposed is the *Commercial Facial Recognition Privacy Act of 2019* (CFRPA),

---

63. *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:30 *Biometrics and State Legislation: An Overview*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).

64. The term "commercial" refers to business uses of the collection of biometric data. For example, commercial uses would pertain to typical stores such as Target, Walmart, or Home Depot, and their use of technology that obtains and compiles biometric data. *See generally* Section I(C) for a discussion of current uses of technology that obtains biometric information.

65. The term "governmental use" refers to all government use including federal, state, and local governments. Governmental use is use of technology that obtains and compiles biometric data for purposes of stopping crime. Governmental use is the focus of this note.

66. *See generally* Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/15 (2016); Texas Biometric Identifiers, Tex. Bus. & Com. Code Ann. § 503.001 (West 2015)(regulating commercial entity collection and use of biometric data); Washington Biometric Identifiers, Wash. Rev. Code Ann. § 19.375.020 (West Supp. 2020).

67. *See generally* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, §§ 31:30.10 *Illinois: Biometric Information Privacy Act*, 31:30.20 *Texas: Capture or Use of Biometric Identifier Act*, 31:30.30 *Washington: Biometric Identifiers Statute*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019) (describing how Illinois enacted comprehensive biometric legislation and other states soon began to follow suit), FISHMAN & MCKENNA, *supra* note 63.

68. FISHMAN & MCKENNA, *supra* note 63; FISHMAN & MCKENNA, *supra* note 67, §§ 31:30.10, 31:30.20, 31:30.30.

69. *See* FISHMAN & MCKENNA, *supra* note 63.

which like state law, only regulates commercial use of facial recognition technology.[70] The CFRPA specifically exempts governmental use of this technology.[71] After discussing state law, this note's discussion will turn to address the current state of the CFRPA and its key provisions.

A. Illinois' Biometric Privacy Information Act ("BIPA")

Illinois became the first state to pass a comprehensive biometric data privacy statute when it adopted the Illinois Biometric Information Privacy Act (BIPA).[72] Illinois enacted BIPA in response to major national corporations choosing the city of Chicago as pilot test sites for the use of biometric facilitated transactions.[73]

BIPA idealized obviating the likelihood of biometric transactions with the ultimate goal of providing for the "public welfare, security, [and] safety, [which would] be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[74] The Illinois law governs two specific categories of data: "biometric identifiers" and "biometric information."[75] The first category of biometric identifiers includes data such as a fingerprint, facial geometry, and a retina or iris scan.[76] The latter category, biometric information, "means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[77]

BIPA makes it illegal for a private entity to obtain a person's biometric identifier or information unless the entity: (1) informs the person in writing that his or her biometric information is being collected or stored; (2) discloses the specific purpose and length for which the data is being collected and stored; and (3) receives a written release from that person to collect and store his or her biometric data.[78]

If and after the requirements for obtaining biometric data have been met, private entities must still meet stringent requirements regarding the

---

70. Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/847/text [https://perma.cc/G46D-MUVJ].

71. *Id.* at § 2(3)(B)(i)–(iv).

72. *See* FISHMAN & MCKENNA, *supra* note 67, §§ 31:30.10, 31:30.20, 31.30.30; FISHMAN & MCKENNA, *supra* note 63.

73. FISHMAN & MCKENNA, *supra* note 67, § 31:30.10.

74. *Id.*

75. *See* 740 ILL. COMP. STAT. ANN. 14/10 (Illinois Biometric Information Privacy Act) (West 2008).

76. 740 ILL. COMP. STAT. ANN. 14/10.

77. 740 ILL. COMP. STAT. ANN. 14/10.

78. 740 ILL. COMP. STAT. ANN. 14/15(b)(1)–(3).

disclosure of the obtained data.[79] First, these private entities may not "sell, lease, trade, or otherwise profit from a person's biometric identifier or biometric information."[80] Second, the private entity may not "disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information" unless: (1) the person consents to the disclosure; (2) the subject requests or authorizes a financial transaction, the completion of which requires the disclosure of biometric data; (3) the disclosure is required by State or federal law or municipal ordinance; or (4) the disclosure is required pursuant to a valid warrant or subpoena.[81]

The underlying goal of BIPA is to ensure transparency with consumers regarding private entities obtaining this information and the information's use.[82] Because of this objective, BIPA further requires these private entities to establish and publicize a written policy for retention of the information and guidelines for which the information is to be destroyed, which at the longest, can be stored for three years.[83] Moreover, the storage of this data must be sufficiently protected from the eyes of third parties, just as any other confidential information would be protected.[84]

BIPA creates a private right of action for "any person aggrieved" by violations of the Act.[85] The penalty imposed on the private entities varies and increases in degree. The degree of the penalty depends on the private entity's culpability, that is, the requisite mental state of the actor. For example, the penalty will be lower if the actor is found to have acted negligently, as opposed to recklessly or intentionally.[86] The Act further allows for other forms of relief, including injunctive relief.[87]

B. Subsequent State Law Development

Other states have begun to follow Illinois' steps in regulating the commercial use of technology that collects and retains biometric information. Among the other states that have since undertaken these regulating efforts, Texas and Washington are two other states that have developed comprehensive biometric legislation. In many respects, the Texas and Washington acts are very similar to BIPA, Illinois' biometric legislation. In other regards, they do have some distinguishing provisions which are worth mentioning.

---

79. *See* 740 ILL. COMP. STAT. ANN. 14/15(c).
80. 740 ILL. COMP. STAT. ANN. 14/15(c).
81. 740 ILL. COMP. STAT. ANN. 14/15(d)(1)–(4).
82. *See* FISHMAN & MCKENNA, *supra* note 67, § 31:30.10.
83. 740 ILL. COMP. STAT. ANN. 14/15(a); s*ee also* FISHMAN & MCKENNA, *supra* note 67, § 31:30.10.
84. 740 ILL. COMP. STAT. ANN. 14/15(e)(1).
85. 740 ILL. COMP. STAT. ANN. 14/20.
86. *See* 740 ILL. COMP. STAT. ANN. 14/20(1)–(2).
87. 740 ILL. COMP. STAT. ANN. 14/20(4).

Texas enacted the Capture or Use of Information Identifier Act (CUBI) in 2009, one year after Illinois enacted BIPA.[88] CUBI is similar to BIPA in that CUBI generally prohibits private commercial entities from collecting, compiling, and retaining an individual's biometric data unless otherwise first notifying and obtaining consent to the data collection.[89] CUBI differs from BIPA in four main respects. First, CUBI does not require notice and consent to be in writing.[90] Second, CUBI does not require private entities to disclose the purpose for collection of the biometric data.[91] Third, CUBI does not require the private entity to specify how long the data will be stored.[92] Fourth, unlike BIPA, CUBI does not provide a private right of action for violations of the Act and instead only allows the Texas Attorney General's Office to recover civil penalties.[93]

Washington was the third state to follow Illinois and Texas' footsteps by passing legislation in 2017 to regulate biometric data and the commercial use and collection of the data.[94] Washington's law is largely similar to BIPA and CUBI. Like BIPA and CUBI, the Washington Act requires notice and consent before biometric identifying information may be stored for a commercial purpose or sold to third-parties.[95] Washington law differs from BIPA in that it does not provide for a private right of action.[96] Instead, the Washington law is similar to CUBI which only permits the attorney general's office to bring causes of action based upon statutory violations.[97]

Other states continue to make significant strides in enacting legislation that would regulate the use and collection of biometric data, either through a biometric-specific statute or by amending existing legislation to provide protection.[98] Among these states include Alaska,

88. FISHMAN & MCKENNA, *supra* note 67, § 31:30.20.

89. TEX. BUS. & COM. CODE ANN. § 503.001(b)(1)–(2).

90. *See generally* TEX. BUS. & COM. CODE ANN. § 503.001(a)–(e) (lacking a notice provision and written consent provision).

91. *See generally* TEX. BUS. & COM. CODE ANN. § 503.001(a)–(e) (lacking a disclosure of purpose provision).

92. *See* TEX. BUS. & COM. CODE ANN. § 503.001(b)–(c); *but see* TEX. BUS. & COM. CODE ANN. § 503.001(c)(3) (requiring that biometric identifying information be destroyed "within a reasonable time" but no later than one year after the expiration of the purpose for collection of the information).

93. TEX. BUS. & COM. CODE ANN. § 503.001(d). It is worth noting as well that the Texas civil penalties are much higher than those provided for in BIPA. CUBI provides for remedies of $25,000 per each violation by a commercial entity.

94. *See* FISHMAN & MCKENNA, *supra* note 67, § 31:30.30.

95. WASH. REV. CODE ANN. § 19.375.020(1)–(3).

96. WASH. REV. CODE ANN. § 19.375.030(2).

97. WASH. REV. CODE ANN. § 19.375.030(2).

98. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 31:32 *Pending Legislation, in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).

California, Idaho, Massachusetts, and New York.[99] Similar to BIPA, CUBI, and the Washington Act, all states seek to provide a general prohibition against the commercial collection and use of biometric data without some form of notice and consent.[100] The differences that do exist among other state-proposed legislation relate to the scope of the definitions of certain terms relating to biometric identification and the requisite penalties for violation of the statute.[101]

C. Proposed Federal Law: Commercial Facial Recognition Privacy Act of 2019 ("CFRPA")

Congress has followed the footsteps of Illinois, Texas, and Washington. On March 14, 2019, Senator Roy Blunt introduced the *Commercial Facial Recognition Privacy Act of 2019* bill, a proposed law that would regulate the collection and use of biometric information in the *commercial* setting.[102] As of current, the bill has been read twice and has since been referred to the Committee on Commerce, Science, and Transportation.[103]

The Act's objective is to "prohibit certain entities from using facial recognition technology to identify or track an end user without obtaining the affirmative consent of the end user . . . ."[104] Unlike the aforementioned state laws, CFRPA provides protections against only the commercial use of facial recognition technology, not other technologies, which is much narrower in scope than state laws like BIPA and CUBI.[105] However, in many respects, CFRPA is similar to BIPA and CUBI. Like BIPA and CUBI, CFRPA focuses only on *commercial* use, collection, and compilation of biometric identifying information by private entities through the use of facial recognition technology.[106] Importantly, the regulation excludes the federal government, state and local government, national

99. *Id.*

100. *Id.*

101. *Id.*

102. Commercial Facial Recognition Privacy Act of 2019, S. 847, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/847/all-actions?overview=closed&KWICView=false (last visited Jan. 19, 2020) [https://perma.cc/3G2C-VCRF].

103. *Id.*

104. *See id.* (stating "[t]o prohibit certain entities from using facial recognition technology to identify or track an ender user without obtaining the affirmative consent of the end user, and for other purposes.").

105. *Id.*

106. *Id.* § 2(3) (defining "covered entities" to include only commercial businesses).

security agency, and intelligence agency uses of facial recognition technology.[107]

CFRPA provides that it is unlawful for a private entity to knowingly use facial recognition technology to collection facial recognition data unless the private entity first obtains "affirmative consent."[108] The Act defines "affirmative consent" to be an "individual, voluntary, and explicit agreement to the collection and data use policies of [] [private entity]."[109] "To the extent possible, if facial recognition technology is present," the private entity must provide the person with notice that facial recognition technology is being used.[110] Included with the notice must be documentation that provides general information regarding the capabilities and limitations of the facial recognition technology.[111] Once information is obtained, private entities are not allowed to share the data with an "unaffiliated third party" without receiving "affirmative consent," separate from the affirmative consent already required to collect biometric identifying information through facial recognition technology.[112]

With regard to providing information about the notice, private entities must describe the specific practices regarding the collection, storage, and use of facial recognition data.[113] This description must include the purpose for collection of the data, the process for data retention, and the ability to review or correct, if any, the information obtained.[114]

Enforcement of the CFRPA is slightly larger in scope than those provisions contained in BIPA and CUBI because the CFRPA has the federal law component. A violation of the general prohibitions mentioned above[115] are treated as violations of unfair or deceptive acts of trade as defined by the Federal Trade Commission Act.[116] CFRPA further provides that attorneys general of the state may bring a civil action on behalf of the residents of the state to seek "appropriate relief."[117]

States and the federal government have taken significant strides to regulate the collection and compilation of biometric identifying information by commercial businesses, exemplifying the idea that such unregulated compilation of information implicates privacy concerns. Accordingly, the question arises of whether unregulated governmental collection and compilation of biometric data similarly implicates the same privacy

107. S. 847 § 2(3)(B)(i)–(iv).
108. S. 847 § 3(a)(1)(A).
109. S. 847 § 2(1).
110. S. 847 § 3(a)(1)(B)(i).
111. S. 847 § 3(a)(1)(B)(ii).
112. S. 847 § 3(a)(4).
113. S. 847 § 3(b)(1).
114. S. 847 § 3(b)(1)(A)–(C).
115. *See* S. 847 § 3.
116. S. 847 § 4(a)–(b)(1)–(2).
117. S. 847 § 4(c)(1).

concerns afforded by Fourth Amendment protections. Section III briefly provides an overview of Fourth Amendment law, and Section IV explores whether this unregulated use violates Fourth Amendment protections.

III. FOURTH AMENDMENT TESTS AND REQUIREMENTS

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[118] These words enumerated within the text of the Fourth Amendment are words of limitation.[119] Whereas the Fourth Amendment only applies to actions taken by state actors, law enforcement practices are not required to be reasonable unless a "search" or "seizure has occurred."[120] Therefore, a discussion on "what police activities, under what circumstances and infringing upon what areas and interests, constitute either a search or seizure within the meaning of that Amendment" [121] is essential in determining whether the Fourth Amendment is implicated through unregulated governmental use of facial recognition technology and the compilation of biometric data.

At the outset, defining a "seizure" under the Fourth Amendment context has not been a source of difficulty that courts have had to grapple with.[122] Generally, a "seizure" occurs within the meaning of the Fourth Amendment when a state actor acts by "physically taking and removing tangible personal property."[123] Along these same lines, the Supreme Court has further stated that a "seizure" of property occurs when "there is some meaningful interference with an individual's possessory interest in that property."[124]

On the other hand, the Supreme Court and lower courts have experienced great difficulty in defining the term "search" within the Fourth Amendment context.[125] Under a traditional approach, the term "search" is said to imply "some exploratory investigation, or an invasion and quest, a look for or seeking out . . . ."[126] In the early 1900's, the Court would define

---

118. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1 at 562 (5th ed. 2012) (quoting U.S. CONST. amend. IV).

119. *Id.*

120. *Id.*

121. *Id.* at 562–63.

122. *Id.* at 563.

123. *Id.* (quoting 68 AM. JUR. 2D SEARCHES AND SEIZURES § 8 (1973)); *see also* Hale v. Henkel, 201 U.S. 43, 76 (1906) (stating that "a seizure contemplates a forcible dispossession of the owner").

124. 1 LAFAVE, *supra* note 118, at 563–64 (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

125. *Id.* at 573.

126. *Id.* (quoting C.J.S., SEARCHES AND SEIZURES § 1 (1952)).

searches as physical intrusions into a "constitutionally protected area."[127] These constitutionally protected areas included areas that were textually enumerated within the Fourth Amendment such as "persons," which would include bodies,[128] clothing,[129] and more. Moreover, "houses" were protected and would include apartments,[130] hotels,[131] garages,[132] and other living arrangements. Where these early Fourth Amendment Court opinions drew largely on property law concepts and physical intrusions of one's property, the traditional property view, as the sole view of Fourth Amendment rights, would change with the Court's "landmark decision"[133] in *Katz v. United States*.[134] *Katz* would rapidly become the basis of a new test[135] for determining what was a "search" within the meaning of the Fourth Amendment and would expand the coverage of the Fourth Amendment.[136] *Katz* would be the dominating standard for over fifty years until 2013, where the historic property-based approach for determining what actions amounted to a "search" would make its return in *United States v. Jones*.[137] Current Fourth Amendment law requires application of both the *Katz* test and the *Jones* test to determine whether a "search" has occurred, and both tests have been further refined with more recent Court opinions. For these reasons, the analysis below will provide a brief overview of the *Katz* test and the *Jones* test and discuss what is required by both tests to make a government action a "search" within the meaning of the Fourth Amendment.

A. The *Katz* Test

In *Katz v. United States*, FBI agents attached an electronic recording and listening device to a public telephone that was used by Katz.[138] The electronic recording device revealed illegal acts by Katz and led to him being indicted on eight separate counts of transmitting wagering

127. *Id.* at 575 (citing Silverman v. United States, 365 U.S. 505, 510 (1961)); *see also* Berger v. New York, 388 U.S. 41, 44 (1967); Lanza v. New York, 370 U.S. 139, 142–43 (1962).

128. *See* Schmerber v. California, 384 U.S. 757, 772 (1966).

129. *See* Beck v. Ohio, 379 U.S. 89, 90, 97 (1964).

130. *See* Clinton v. Virginia, 377 U.S. 158, 158 (1964).

131. *See* Stoner v. California, 376 U.S. 483, 490 (1964).

132. *See* Taylor v. United States, 286 U.S. 1, 6 (1932).

133. 1 LAFAVE, *supra* note 118, at 576 (quoting Michael D. Granston, Note, *From Private Places to Personal Privacy: A Post-Katz Study of Fourth Amendment Protection,* 43 N.Y.U. L. REV. 968, 968 (1968)).

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

135. 1 LAFAVE, *supra* note 118, at 580.

136. *Id.* at 582.

137. *See* United States v. Jones, 565 U.S. 400 (2012).

138. *Katz*, 389 U.S. at 348.

information.[139] On writ of certiorari, Katz challenged the constitutionality of the government's use of the electronic recording device and argued that use of the device constituted a "search" and violated his Fourth Amendment protections against unreasonable searches.[140]

The Court agreed, finding that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[141] Justice Harlan, concurring, would formulate a two-part test, the *Katz* test, that would come to be used by the Court over the course of the next fifty years and is still in use today.[142] The two-part test for determining whether a search has occurred in the context of the Fourth Amendment requires that: (1) the aggrieved person has demonstrated an actual (subjective) expectation of privacy; and (2) the expectation of privacy must be one that society is prepared to recognize as "reasonable."[143] The Court, in subsequent decisions, has further expanded upon both requirements of the *Katz* test.

1. Requirement One: Demonstrating an Actual Subjective Expectation of Privacy

Since the *Katz* opinion, the Court has done little to distinguish between the two parts of the *Katz* test.[144] It is true that, often, the issue is not raised, but the Court has stated in dicta that part one of the *Katz* test requires that an individual demonstrate that she has taken affirmative steps to ensure privacy from unwarranted surveillance.[145] For example, in *Ciraolo v. California*, the defendant was growing marijuana in his back yard which was surrounded by fences blocking view from the public road, but still capable of being seen from an aerial viewpoint.[146] Chief Justice Burger, writing for the Court, stated in dicta that part one of the *Katz* test in this case likely would have required a showing that a defendant has taken all affirmative steps to ensure against all conceivable efforts of scrutiny by

139. *Id.*

140. *Id.* at 348–49.

141. *Id.* at 353.

142. *Id.* at 361; *see also* 1 LAFAVE, *supra* note 118, at 579 (noting how Justice Harlan's concurring two-fold test quickly became relied upon by lower courts in addressing Fourth Amendment cases).

143. *Katz*, 389 U.S. at 361.

144. 1 LAFAVE, *supra* note 118, at 584 (citing Eric Dean Bender, *The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?*, 60 N.Y.U. L. REV. 725, 744–45 (1986)).

145. *See* California v. Ciraolo, 476 U.S. 207 (1986).

146. *Id.* at 209–10.

the government.[147] The implication of this comment is that if the issue is raised, a defendant will likely need to demonstrate that she has taken steps to ensure against all conceivable efforts of scrutiny by the government.[148] Therefore, it is likely appropriate to ponder hypothetical occurrences to determine if a defendant has taken steps to protect her privacy and thus sufficiently pass the first hurdle of the *Katz* test.[149]

2. Requirement Two: An Expectation That Society is Prepared to Recognize as Reasonable

The second factor of the *Katz* test, as mentioned above, requires the Court to find that a person's subjective expectation of privacy be one that society is prepared to recognize as "reasonable."[150] In other words, the second prong of the *Katz* test asks whether the expectations of privacy are constitutionally "justifiable."[151] What is "justifiable" turns on the context of the intrusion.[152] Justice Harlan further described the second prong by writing in his dissent in *United States v. White* that "[t]he question must be answered by assessing the nature of a particular practice and the likely extent of its impact on the individual's sense of security balanced against the utility of the conduct as a technique of law enforcement."[153] Being faced with varying factual situations and differing technological uses by the government has required the Court to look for the answer to the second prong by analyzing the structure of society, the patterns of interaction, and the web of norms and values.[154] As the Court noted in *Oliver v. United States*, the inquiry is based on a "societal understanding" of what "deserves protection from government invasion."[155]

The Court, in applying the second prong, does not stop with societal expectations, but also makes a judgement with respect to whether the investigative practice in question threatens a "sense of security."[156] This

147. *Id.* at 211–12. It should be clarified that on appeal, the State did not argue to the Court that Ciraolo had failed to demonstrate a subjective expectation of privacy; however, Chief Justice Burger reasoned there was a question as to whether Ciraolo demonstrated a subjective expectation of privacy from *all* observations of his backyard.

148. 1 LAFAVE, *supra* note 118, at 585.

149. *Id.*

150. *See* Katz v. United States, 389 U.S. 347, 361 (1967).

151. *Id.* at 353.

152. 1 LAFAVE, *supra* note 118, at 586.

153. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

154. 1 LAFAVE, *supra* note 118, at 587 (quoting Arnold Simmel, *Privacy Is Not an Isolated Freedom*, *in* NOMOS XIII: PRIVACY, at 71, 84 (J. Pennock & J. Chapman eds. 1971)).

155. Oliver v. United States, 466 U.S. 170, 178 (1984).

156. 1 LAFAVE, *supra* note 118, at 589.

inquiry requires viewing the case at hand from a broad perspective, which ultimately asks whether permitting the police regularly to engage in the specific type of practice requires citizens of the United States to give up "too much freedom as the cost of privacy."[157] Moreover, the question becomes one that asks if the encroachment on privacy would be intolerable because it would impede too much upon the sense of security of persons who wished to maintain that security.[158] Since *Katz* was written, the Court has further expanded the *Katz* test and has adopted more nuanced Fourth Amendment doctrines[159] under the *Katz* test as it relates to privacy protections. Of importance to this note is a discussion on Fourth Amendment implications through a state actor's ongoing surveillance of an individual's relationships and movements. These concerns are addressed next.

3. Ongoing Surveillance in the Context of the Katz Test

Depending on the type of investigation, law enforcement will sometimes engage in ongoing surveillance of movements and relationships in public.[160] Generally, fixed surveillance may be used for a period of time in an effort to uncover evidence of criminal activity.[161] Moving surveillance may be conducted briefly or for a period of several months in order to determine if an individual has engaged in criminal activity.[162]

Use of publicly available information about the individual has historically been seen as not violating a Fourth Amendment right,[163] and thus does not constitute a search or seizure, because "what a person knowingly exposes to the public is not a subject of Fourth Amendment protection."[164] As earlier Fourth Amendment cases often noted, surveillance

157. *Id.* (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment,* 58 MINN. L. REV. 349, 403 (1974)).

158. *Id.*; *see also* Amsterdam, *supra* note 157, at 402 (1974) ("[T]his approach raises the question of how tightly the fourth amendment permits people to be driven back into the recesses of their lives by the risk of surveillance.").

159. There are many other Fourth Amendment doctrines that are vastly important but are outside the scope of this note. Among other various Fourth Amendment doctrines that will not be mentioned in this note include: the "open fields" doctrine; the "container" doctrine; and the "third-party" doctrine.

160. 1 LAFAVE, *supra* note 118, at 1015.

161. *Id.*

162. *Id.*

163. *Id.* at 1016 (citing George C. Christie, *Government Surveillance and Individual Freedom: A Proposed Statutory Response to* Laird v. Tatum *and the Broader Problem of Government Surveillance of the Individual*, 47 N.Y.U. L. REV. 871, 885 n.68 (1972)).

164. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

of public movements is not protected because there is no reasonable expectation of privacy[165] in such movements.[166]

However, the Court has found issue with use of investigative technology that is used to gather and compile information on an individual over a large span of time. The Court first noted, in dicta, in *United States v. Knotts* that continual surveillance by the government could constitute a search.[167] In *Knotts*, the government placed a "beeper" in a container of chloroform purchased by a trio of co-defendants including Knotts.[168] From the initial purchase, the government followed the "beeper" in the chloroform container to an out-of-state, secluded cabin, which upon search revealed a large drug operation.[169] Before the Court, Knotts argued that the surveillance of the beeper's whereabouts on public roads constituted a search, the search was unreasonable, and thus the search violated his Fourth Amendment protections.[170] Writing for the Court, Chief Justice Rehnquist disagreed with Knotts and held that no search had occurred, and thus there was no violation of Knotts's Fourth Amendment protections.[171]

Although the *Knotts* Court determined there was no search under the Fourth Amendment because the beeper tracking that occurred took place over public thoroughfares, the majority still discussed that there would potentially be a Fourth Amendment issue had the government constantly surveyed Knotts's public movements over the course of twenty-four hours.[172] Disposition of this issue would be left for another day.

Concerns over constant surveillance were readdressed in *United States v. Jones*.[173] In *Jones*, the Court addressed privacy implications of the attachment of a GPS monitoring device to a vehicle driven by Jones over the course of twenty-eight days.[174] Justice Scalia, writing for the Court, would apply a separate test from *Katz* (expanded on below in the next section), but five Justices,[175] concurring in the judgment, reasoned that the continual twenty-eight day surveillance violated the *Katz* test.[176] Justice

---

165. *Supra* Section III(A)(2) (discussing reasonable expectation of privacy under *Katz*).

166. *See Katz*, 389 U.S. at 511; Cardwell v. Lewis, 417 U.S. 583, 590–91 (1974).

167. United States v. Knotts, 460 U.S. 276, 283–84 (1983).

168. *Id.* at 278.

169. *Id.* at 278–79.

170. *Id.* at 284.

171. *Id.* at 285.

172. *Id.* at 283–84.

173. *See* United States v. Jones, 565 U.S. 400 (2012).

174. *Id.* at 404.

175. *See id.* at 413–31 (Sotomayor, J., concurring in the judgment finding a violation of *Katz*. Alito, J., joined by Ginsberg, J., Breyer, J., and Kagan, J., concurring in the judgment also finding a violation of *Katz*).

176. *Id.* at 404–05 (Scalia, J., applying the trespass-based test and holding there was a "search" within the meaning of the Fourth Amendment).

Sotomayor, concurring in the judgment, agreed with the majority approach, but reasoned that the twenty-eight day surveillance by the government additionally violated *Katz* since "long term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[177] Even in cases of short-term monitoring, Justice Sotomayor felt that use of constant surveillance "will require particular attention."[178] Cases with continuous government surveillance implicated privacy concerns because GPS monitoring and other newer technologies are capable of obtaining a "wealth of detail about . . . familial, political, professional, religious, and sexual associations."[179] Left unregulated, Justice Sotomayor recognized that the government can store these records and effectively mine the records for information for years.[180] Moreover, because technologies like GPS monitoring are cheap and efficient, they were capable of evading normal checks on abusive law enforcement practices.[181]

The same concerns of long-term surveillance were readdressed by the Court in *Carpenter v. United States*.[182] In *Carpenter*, the Court held that the government's procurement of cell-site location information (CSLI) that showed Carpenter's cell phone movement and location over the course of seven days violated the *Katz* test.[183] The *Carpenter* case involved a valid federal magistrate judge order that required Carpenter's cell phone carriers to produce collectively 152 days' worth of CSLI from one mobile carrier and seven days' worth from another mobile carrier.[184]

Writing for the Court, Chief Justice Roberts relied upon the distinctions made in *Knotts* and *Jones*. Similar to the concerns voiced by Justice Sotomayor in her concurring opinion in *Jones*,[185] Chief Justice Roberts emphasized how the CSLI records obtained by the government provided an "all-encompassing record of the holder's whereabouts."[186] Similar to the GPS device used in *Jones*, the CSLI records were time stamped data that provided an "intimate window into a person's life."[187] Such location records "hold for many Americans 'the privacies of life.'"[188]

Chief Justice Roberts raised an issue with the retrospective quality of the data obtained in *Carpenter* as well.[189] Because the CSLI records were

177. *Id.* at 415.
178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.* at 415–16.
182. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
183. *Id.* at 2219.
184. *Id.* at 2212.
185. *See Jones*, 565 U.S. at 415.
186. *Carpenter*, 138 S. Ct. at 2217.
187. *Id.*
188. *Id.* (citing Riley v. California, 134 S. Ct. 2473, 2494–95 (2014)).
189. *Id.* at 2218.

compiled and maintained over the course of years, the police had all access to reconstruct a person's movements, allowing for the ability to "travel back in time" without needing to know in advance which individual they wanted to follow.[190] What this effectively turned out to be, as Chief Justice Roberts explained, is that an individual has been "tailed every moment of every day for five years."[191] The *Carpenter* opinion is one that the Court adopted and felt that it must hold in order to "take account of more sophisticated systems that are already in use or in development."[192]

As the above discussion reflects, the *Katz* standard is a test that has been highly litigated and has numerous facets to it depending on the context and duration of the investigative procedure implemented by government authorities. Although seemingly more developed, the *Katz* test is not the only test that the Court has applied in determining whether a government action has resulted in a "search" or "seizure" under the Fourth Amendment. The second test is the *Jones* test, which is expanded upon in the next section.

B. The *Jones* Test

As briefly discussed above, the *Katz* test was the sole Fourth Amendment "search" test over the past fifty years, but as of 2013, in the opinion of *United States v. Jones*,[193] the Court revived a past approach to determining whether a government action is a "search" that is based on traditional "trespass" law.[194] This second test is referred to as the *Jones* test, and like *Katz*, if the test is satisfied, then the government's action constitutes a "search" within the meaning of the Fourth Amendment. *United States v. Jones* involved a reexamination of the trespass doctrine–which prior to the Court's opinion in *Katz* was the standard applied by the Court in addressing whether a Fourth Amendment "search" or "seizure" has occurred.[195] *Jones* involved the government's installation of a GPS tracking device on the undercarriage of a vehicle used by Jones.[196] Jones would then use this car over the course of the next twenty-eight days where the government would track every single movement of the vehicle.[197] All nine

190. *Id.*

191. *Id.*

192. *Id.* (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).

193. United States v. Jones, 565 U.S. 400, 405 (2012).

194. 1 LAFAVE, *supra* note 118, at 593.

195. *See Jones*, 565 U.S. at 405–06 (Scalia, J., describing how prior to *Katz*, Fourth Amendment protections were tied to common-law trespass).

196. *Id.* at 402–03.

197. *Id.*

Supreme Court Justices would agree that this action constituted a search, but not all Justices would agree as to how that holding was reached.[198]

The majority did not apply the *Katz* test, for a person's "Fourth Amendment rights do not rise or fall with the *Katz* formulation."[199] Her rights do not rise or fall with *Katz* because the "*Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test." Therefore, as the majority reasoned, it was enough to show that the "[g]overnment physically occupied private property for the purpose of obtaining information [with] such a physical intrusion . . . [constituting] a 'search' within the meaning of the Fourth Amendment when it was adopted."[200]

Based on the majority's holding, the *Jones* test can be broken into three factors. First, did the government physically intrude or trespass on property?[201] Second, was the intrusion by the government into an area protected by the Fourth Amendment (persons, houses, papers, effects)?[202] Third, did the government intrude on this protected area to obtain information? If these three factors are met, then a "search" has occurred under the *Jones* test.[203]

The *Jones* test was further refined in *Florida v. Jardines*.[204] *Jardines* refined the *Jones* test by adding another element to the mix. Based on the holding in *Jardines*, future application of the *Jones* test requires lower courts to ask whether the officer's investigation was accomplished through an unlicensed physical intrusion.[205] Based on the *Jardines* holding, courts now look to see whether the physical intrusion into the curtilage of a homeowner's property extends beyond the implicit license that the homeowner allows potential visitors.[206] In *Jardines*, the Court acknowledged that an implicit license is provided to both welcome and unwelcome visitors.[207] This means that an implicit license will be found to extend to friends, relatives, mail carriers, solicitors, peddlers, and others of

198. *See id.* at 400. All Justices would agree this was a "search" within the meaning of the Fourth Amendment. Justice Sotomayor, concurring, believed that the majority could have additionally applied *Katz* and that the government's actions would have constituted a "search" under *Katz*. Justice Alito, concurring, felt that the Court should not have revived the trespass doctrine and instead only applied *Katz* which would have led to the holding that this was a "search."

199. *Id.* at 406.

200. *Id.* at 404–05.

201. *Id.* at 404.

202. *Id.* at 407.

203. *Id.* at 404.

204. *See* Florida v. Jardines, 569 U.S. 1 (2013).

205. *See id.*

206. *Id.* at 8–9.

207. *Id.* at 9.

the like.[208] This holding comes with its limits. For one, the implicit license is spatially limited.[209] The *Jardines* Court noted that the implicit license extends to allow visitors to approach a home by the front entrance, as opposed to making "circuitous detours that veer from the pathway that a visitor would customarily use."[210]

The *Jardines* Court further provided that this rule has its temporal limits.[211] Ultimately, a visitor has an implicit license to knock promptly, wait to be received, and then (absent an invitation to linger longer) leave."[212] Thus, an officer's presence may exceed any implicit license merely because of the length of time spent there, such that even plain-view situations arising thereafter become unlawful searches.[213]

The main distinction between the *Katz* test and the *Jones* test is one of expectations of privacy versus physical encroachment upon protected areas. Under *Katz*, courts are called to make subjective determinations as to whether reasonable expectations of privacy have been violated; a *Katz* "search" can occur regardless of a physical intrusion by government officials or government investigative technology. The *Jones* test, instead, focuses on whether the government officials or technology has exceeded unlicensed physical intrusions by the government into constitutionally protected areas. Whether the government's use of facial recognition technology to obtain and compile biometric data violates the *Katz* test or *Jones* test is discussed next.

IV. FOURTH AMENDMENT IMPLICATIONS OF GOVERNMENTAL USE OF FACIAL RECOGNITION TECHNOLOGY THAT COMPILES AN INDIVIDUAL'S BIOMETRIC DATA

As discussed earlier, current state law and the proposed federal law, the Commercial Facial Recognition Privacy Act of 2019 ("CFRPA"), do not regulate the governmental use of facial recognition technology, nor the compilation of biometric data on individuals through the use of facial recognition technology.[214] Based on Fourth Amendment case law, the unregulated governmental use of such technology that compiles biometric data is an unreasonable "search" and violates the *Katz* test. Discussion below first analyzes the Fourth Amendment implications of compilation of biometric data and the *Katz* test. Following the *Katz* test discussion is analysis on the *Jones* test implications of biometric data compilation by governmental entities.

208. *Id.* at 8.
209. *See id.* at 9.
210. *Id.* at 19 (Alito, J., dissenting).
211. *Id.* at 8.
212. *Id.*
213. *Id.*
214. *See supra* Sections II(A)–(C).

A. Compilation of Biometric Data Through Governmental Use of Facial Recognition Technology is an Unreasonable "Search" Under the *Katz* Test

Unregulated governmental use of facial recognition technology which maintains a database of biometric data violates the *Katz* test because the compilation of biometric data violates all American citizens' subjective expectations of privacy. Recall that *Katz* requires a two-fold test be met in order for the government action to be considered a search. The two-part test for determining whether a search has occurred under *Katz* requires asking: (1) the aggrieved person has demonstrated an actual (subjective) expectation of privacy; and (2) the expectation of privacy must "be one that society is prepared to recognize as 'reasonable.'"[215]

First, American citizens demonstrate a subjective expectation of privacy in the belief that the government will not constantly survey and compile every movement and location. This expectation of privacy extends not only to what is done in the home, where privacy protections are at their highest,[216] but as well to areas out in public, to activities that the person seeks to preserve as private.[217] Recall in *Katz*, where the Court held that Katz's expectations of privacy had been violated where he had "justifiably relied" on the belief that the contents of his phone call–made at a public pay phone–would remain private.[218] It is oft quoted that "what a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection,"[219] but the *Katz* Court found a violation of expectations of privacy by Katz.[220] What was of importance to the *Katz* Court was not the fact that the telephone call occurred in public, but that regardless of its public nature, Katz sought to keep the contents of his phone call private.[221] For "wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[222]

These same foundational principles enumerated in *Katz* have consistently been applied by the Court in addressing cases involving the government's use of technology to track movements, obtain, and compile information over a course of time. Recall *Jones*, where Justice Alito, concurring in the Court's judgment, expanded upon how use of longer term GPS monitoring (or in this case facial recognition technology) impinges

215. Katz v. United States, 389 U.S. 347, 361 (1967).

216. *See* Oliver v. United States, 466 U.S. 170, 178 ("The overriding respect for the sanctity of the home that has been embedded in our traditions since the origins of the Republic").

217. *Katz*, 389 U.S. at 353.

218. *Id.*

219. *Id.* at 352–53.

220. *Id.*

221. *Id.* at 359.

222. *Id.*

upon expectations of privacy.[223] The fact that such GPS monitoring violates, as a whole, society's general expectation that their movements will not be tracked and recorded over a period of time turns on the historical nature of the ability of law enforcement to investigate crimes.[224]

Past law enforcement practices made it to where officers simply could not secretly "monitor and catalogue every single movement of an individual's car for a very long period of time."[225] Prior to the digital age, law enforcement may have pursued a suspect for a brief stretch but pursuing for a long period of time was difficult, costly and rarely undertaken.[226] These same concerns were voiced in *Carpenter*. Even in *Carpenter*, where the petitioner willingly provided his location information to the mobile carriers (implicating the third-party doctrine),[227] the Court held that obtaining the CSLI data displaying Carpenter's movements over days of time contravened his expectations of privacy.[228]

Consistent with these opinions, American citizens at the very least have a reasonable expectation of privacy in keeping their biometric identifying information, and derivative locational whereabouts, free from a government's surreptitious compilation of such information.[229]

Second, this general expectation of privacy is one that society is prepared to recognize as reasonable. A general expectation that the government will not catalogue an individual's biometric identifying information, revealing her location at any and all times, is one that is "justifiable"[230] in light of considering "the impact on the individual's sense of security."[231] Such unregulated use of facial recognition technology and compilation of biometric data requires American citizens "to give up too much freedom at the cost of privacy."[232] Ultimately, an individual's

---

223. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

224. *Id.* at 430.

225. *Id.*

226. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

227. *See generally* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976). Discussion of the third-party doctrine is outside the scope of this note, but generally, information provided to third parties is not protected by the Fourth Amendment. It is reasoned that individuals have no expectation of privacy in this information they voluntarily convey to third parties.

228. *Carpenter*, 138 S. Ct. at 2217–18.

229. *Id.* at 2217 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring)). It should be noted that the Court has yet to define a line as to what duration of length of surveillance violates expectations of privacy. Based on the holding in *Carpenter*, constant surveillance that is seven days, or longer, violates reasonable expectations of privacy.

230. Katz v. United States, 389 U.S. 347, 353 (1967).

231. United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

232. 1 LAFAVE, *supra* note 118, at 589 (quoting Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974)).

biometric data and physical movements is one that "deserves protection from government invasion,"[233] and past Court precedent bolsters this contention. In considering *Katz*, *Jones*, and *Carpenter*, which involved smaller invasions of privacy expectations than the issue posed in this case, this expectation of privacy is absolutely one that is reasonable.

Third, government use of facial recognition technology that obtains and compiles biometric data is unreasonable absent a valid warrant.[234] Since the current government use of facial recognition technology is not conducted pursuant to a warrant, all unregulated use of this technology is an unreasonable search within the meaning of the Fourth Amendment pursuant to the *Katz* test.

B. Compilation of Biometric Data Through Governmental Use of Facial Recognition Technology Likely Does Not Violate the *Jones* Test Depending on the Location of the Technology

Compilation of biometric data through governmental use of facial recognition technology likely does not violate the *Jones* test. Recall that the *Jones* test requires a physical intrusion into a constitutionally protected area to obtain information.[235] With facial recognition technology, there is likely no actual physical invasion onto a person's property and thus, the *Jones* test would not be implicated.

At least five Justices of the Court would likely agree with this proposition. Both Justice Sotomayor and Justice Alito, concurring in the judgment of *Jones*, discussed how situations involving the transmission of electronic signals would remain subjected to *Katz* analysis.[236] Moreover, as Justice Sotomayor notes in *Jones*, the trespass test offers little guidance in cases involving novel modes of surveillance that do not involve a physical invasion on a person's property.[237] Based on this reasoning, and until the Court provides an extension of the *Jones* test, it is likely that *Jones* would provide little protection. The Fourth Amendment analysis involving electronic surveillance is subjected to a *Katz* analysis.

Past Court precedent demonstrates that individuals have a reasonable expectation of privacy in their movements. Governmental use of facial recognition technology that compiles biometric data of American citizens is an "unreasonable search" within the Fourth Amendment and, thus, should be disallowed.

---

233. Oliver v. United States, 466 U.S. 170, 178 (1984).

234. *See Katz*, 389 U.S. at 357 ("searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment . . . .").

235. United States v. Jones, 565 U.S. 400, 404 (2012).

236. *See id.* at 413–18 (Sotomayor, J., concurring); 418–31 (Alito, J., concurring).

237. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

V. FOURTH AMENDMENT PROTECTIONS ARE NOT ENOUGH: STATUTORY REFORM IS NEEDED

Fourth Amendment rights extend to all American citizens and serve as the lowest form of civil liberties granted, irrespective of federal statutory law or state law. In other words, neither Congress, state legislatures, nor lower courts may abolish any protections afforded by the Fourth Amendment and its interpretative case law. But the Fourth Amendment serves as the bottom line: Congress and the states do have the power to afford greater protections than what is extended by the United States Constitution.

Do we need more protections though? Are there compelling reasons to focus legislative efforts on fashioning comprehensive reform, allowing for greater protections against governmental use of facial recognition technology? If so, what is the best route?

To be sure, there are arguments that lean both ways. We can be confident in knowing that national security, and the need for it, is always of utmost importance. Between terrorism threats, domestic extremism, trade conflicts, cyberattacks, and the always lurking issues over nuclear threats, facial recognition technology provides a valuable means for keeping a watchful eye over subjects thought to pose a threat to America and its people.[238] Yet, the United States' democracy is founded upon individual rights and basic civil liberties; as discussed in detail above, unregulated compilation of a person's biometric data, which provides an all-encompassing record into someone's life, encroaches into protections that are the cornerstone of the United States Constitution. Among these basic rights includes the right to privacy, a right to be free in one's self, free from oppressive government, and unrestricted from overreaching investigative tactics.[239]

Individual liberties weigh strongly in favor of adopting more protections in the form of statutory reform to ensure that an individual's right to privacy is protected. This section proceeds by addressing policy considerations for adopting greater protections to secure privacy rights. After exploring policy concerns, this note shifts gears by proposing statutory protections that draw heavily from the Omnibus Crime Control and Safe Streets Act, otherwise commonly referred to as the Wiretap Act or Title III.

This section will conclude by discussing the strengths in adopting statutory protections and explores the advantages of the legislative branch

238. *See* THIRD WAY, *Talking Points for the Top National Security Issues of 2019* (June 3, 2019), http://thirdway.imgix.net/pdfs/talking-points-for-the-top-national-security-issues-of-2019.pdf [https://perma.cc/R4E3-63XV].

239. *See* ACLU, *The Bill of Rights: A Brief History*, https://www.aclu.org/other/bill-rights-brief-history (last visited Aug. 30, 2020) [https://perma.cc/H5NR-HPQ5].

in fashioning comprehensive statutory protections that ensure privacy, while still allowing for lawful use of governmental use of facial recognition technology and compilation of biometric data, under appropriate measures and standards. The ultimate aim of the statutory proposal is to demonstrate the viability of this measure which would ultimately ensure a much-needed balance between privacy rights and law enforcement needs for use of facial recognition technology in combating crime.

A. Why Do We Need Stronger Privacy Protections Than What is Afforded by the Fourth Amendment?[240]

Fourth Amendment protections are implicated where a state actor uses facial recognition technology to compile an individual's biometric data. From a 30,000-foot view, we can all agree that an always watching camera that records our every movement is concerning and intrusive. But, at the heart of the matter, why do American citizens deserve greater protections against unregulated governmental use of facial recognition technology? How exactly does this technology, and the derivative use of compilation of biometric data, impinge upon our privacy expectations and protections? On a fundamental level, privacy touches the essence of our personhood. Michael McFarland states that, "[r]everence for the human person as an end in itself and as an autonomous being requires respect for personal privacy. To lose control of one's personal information is in some measure to lose control of one's life and one's dignity."[241]

To be sure, Michael McFarland offers five arguments that lend support of adopting more privacy protections. These five arguments will be addressed in turn below and include protection: (1) against misuse of personal information; (2) of relationships; (3) of autonomy; (4) of human dignity; and (5) against boundless government power.

1. Protection and the Misuse of Personal Information

Privacy protections include the need to protect a person against revealing her sensitive personal information. Michael McFarland describes this sensitive personal information as including medical records, psychological tests, court records, financial records, welfare records, internet site records, and other sources that "hold many intimate details of a

240. Another component of privacy rights and constitutional protection is the First Amendment right to freedom of association. Where this section largely touches on First Amendment arguments, the First Amendment right to freedom of association is outside the scope of this note.

241. Michael McFarland, *Why We Care About Privacy*, SANTA CLARA UNIV. (June 1, 2012), https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/why-we-care-about-privacy/ [https://perma.cc/B5N4-B3XH].

person's life."[242] The concern with the government obtaining sensitive information is that it is susceptible to abuse in the form of prejudice and discrimination.[243] McFarland poses a hypothetical to illustrate this point. Consider a situation where others become aware that a person has a history of mental illness. With this knowledge, he could be harassed and shunned by neighbors or employers. Harassment could infiltrate itself into the workplace, subjecting a person to insensitive remarks, serious emotional distress, embarrassment, and prejudice.

The hypothetical posed by McFarland is not a far stretch when we consider the current state of privacy protections in China. Currently, China employs a social credit system to evaluate their citizens.[244] The social credit system, as Business Insider describes it, is a ranking system that ranks every single person based on their "social credit."[245] Projections show that the program is to be fully in operation by 2020 and will be mandatory for every citizen.[246] The exact method that is used to increase or decrease someone's score is unknown, but examples of infractions include unacceptable driving habits, smoking in non-smoking zones, buying too many video games, and posting fake news online (information that would otherwise require obtaining sensitive personal information about payment and website search history).[247]

The social credit system does not merely stand as a number reflecting your value to society: a low social credit number exposes persons to varying levels of punishments.[248] For one, a low social credit number prevents unsatisfactory citizens from flying or traveling by train. It is estimated that nine million China citizens are currently unable to fly domestically due to their inadequate social credit numbers.[249] Others with low social credit numbers are either banned from attending higher education schools, or worse, their blameless children are banned from these programs.[250] For example, in 2018, a Chinese university denied an incoming student a spot for admission due to her father's bad social credit score.[251]

---

242. *Id.*

243. *Id.*

244. Alexandra Ma, *China Has Started Ranking Citizens With a Creepy 'Social Credit' System*, BUS. INSIDER (Oct. 29, 2018, 11:06 AM), https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4 [https://perma.cc/2FGV-KUQ6].

245. *Id.*

246. *Id.*

247. *Id.*

248. *Id.*

249. *Id.*

250. *Id.*

251. *Id.*

Even where some Chinese citizens are lucky enough to escape the consequences of their deficient behavior, in the eyes of the government, citizens can still be sure that there is always the option that they will be publicly shamed for all to see their wrongdoings.[252] Failure to pay a fine or court-ordered compensation, or a default on your debts, will place the substandard citizen on the "list of untrustworthy persons."[253] When these "blacklisted" persons cross certain intersections in Beijing, facial recognition technology projects their face and ID number on massive electronic billboards.[254] China describes this social credit system as an idea that "keeping trust is glorious and breaking trust is disgraceful."[255]

Sure, the Chinese "social credit system" is by all means an extreme example, but the underlying point is this: the social credit system thrives on the government having an individual's personal information. In other words, the social credit system would not be viable without the millions of cameras capturing your substandard driving, one too many cigarettes smoked, or disagreeable eating habits or website viewing habits. If anything, the Chinese social credit system demonstrates the undeniable power of information and the need to preserve privacy protections.

2. Privacy and Relationships

Privacy protections are vital to facilitate social interchange and relationships.[256] James Rachels, in *Why Privacy is Important*,[257] argues that privacy is an essential prerequisite for forming relationships.[258] The strength of the relationship turns on the degree of intimacy between the two persons and the information each are willing to reveal.[259] What personal information is revealed to either a friend or significant other is much different than what one would reveal to an employer or a government entity.[260]

As Rachels points out, relationships of all kinds, be it a close friend or an acquaintance, require a special level of openness and trust that is only possible with assurances that what one reveals will be able to be kept

252. *See* Charlie Campbell, *How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens*, TIME, https://time.com/collection/davos-2019/5502592/china-social-credit-score/ (last visited Jan. 25, 2020) [https://perma.cc/8R2M-CNKD].

253. *Id.*

254. *Id.*

255. Ma, *supra* note 244.

256. McFarland, *supra* note 241.

257. *Id.*; *see also* James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFF. 323 (1975).

258. McFarland, *supra* note 241.

259. *Id.*

260. *Id.*

private.[261] Consider, for example, two distinct relationships: the husband-wife and the therapist-client relationships. Both of these relationships serve much needed goals in society, but both can easily crumble once these persons lose assurance that their revelations will either be disclosed or are capable of being discovered by a third party.[262] Moreover, if we place relationships under constant observation, then persons could not enjoy the degree of intimacy that has been afforded to their relationships over the course of life.[263] Charles Fried states the issue more broadly. Fried writes that privacy is "necessarily related to the ends and relations of the most fundamental sort: respect, love, friendship and trust . . . without privacy they are simply inconceivable."[264]

3. Privacy and Autonomy

McFarland suggests that the analysis from Rachels and Fried reflect a more fundamental issue underlying privacy rights, that is, personal freedom.[265] Deborah Johnson put it as "[t]o recognize an individual as an autonomous being, an end in himself, entails letting that individual live his life as he chooses. Of course, there are limits to this, but one of the critical ways that an individual controls his life is by choosing with whom he will have relationships and what kind of relationships these will be . . . information mediates relationships. Thus, when one cannot control who has information about one, one loses considerable autonomy."[266]

McFarland argues that "los[ing] control of personal information is to lose control of who we are and who we can be in relation to the rest of society."[267] As he writes, "[a] normal person's social life is rich and varied, encompassing many different roles and relationships. Each requires a different *persona*, a different face. This does not necessarily entail deception, only that different aspects of the person are revealed in different roles."[268] Once this personal information becomes controlled over how and to whom it is revealed, an individual loses control over his ability to choose and realize his place in society.[269]

---

261. *Id.*
262. *Id.*
263. *Id.*
264. *Id.*; *see also* Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968).
265. McFarland, *supra* note 241.
266. *Id.*; *see also* DEBORAH G. JOHNSON, COMPUTER ETHICS 65 (Prentice-Hall 1985).
267. McFarland, *supra* note 241.
268. *Id.*
269. *Id.*

4. Privacy and Human Dignity

Autonomy is a smaller characteristic of the broader right to basic human dignity.[270] McFarland suggests that there is an obligation on part of the government and others to treat people not merely as means and data, but as valuable and worthy of respect in themselves.[271] Personal information, ultimately, is an extension of the person, including and encompassing all intimate details of their life.[272] Once others access the intimate and detailed information, they have in essence accessed the person.[273] McFarland argues that where "personal information is taken, sold, or distributed, against the person's will, . . . [his individuality] . . . becomes alienated" and transitions into value as merely a commodity.[274] Essentially, obtaining one's personal information or data treats the person more as an item, and a means to be used for some other end.[275]

5. Privacy and Safeguarding of Freedom Against Boundless Power

Knowledge of an individual's personal information is powerful. Individual privacy is an absolute necessity in order to safeguard the freedom of relationships between individuals, groups, and the government. Alan Westin, in discussing privacy rights, draws attention to the fact that surveillance and publicity are extremely powerful instruments of social control.[276] Once an "individual's actions and dispositions" become publicized, constantly observed, and subjected to comment or criticism, individual expression and association with others becomes suppressed. For where actions are under constant scrutiny, an individual will find it challenging, at best, and fearful, at worst, to stay from social norms and stay true to her individual qualities, characteristics, and beliefs.[277]

Viewed under inspection, the ability to stand alone, to be different, to be individual, becomes frightening, especially where these valuable individual qualities are subject to public criticism.[278] Westin states that the "deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who know his secrets."[279] It is under these circumstances that individuals find it easier to conform to

270. *Id.*
271. *Id.*
272. *Id.*
273. *Id.*
274. *Id.*
275. *Id.*
276. ALAN F. WESTIN, PRIVACY AND FREEDOM (New York: Atheneum 1967).
277. McFarland, *supra* note 241.
278. *Id.*
279. WESTIN, *supra* note 276, at 32.

suggested, or required, social norms as opposed to stand apart in their true beliefs and expressions.[280]

What this means for privacy is that protections from the excessive scrutiny of an overreaching government power are required and are necessary for individuals to "be free to be themselves."[281] The ability of one to develop her unique individuality is especially important in the United States democracy, "which values and depends on creativity, nonconformism and the free interchange of diverse ideas."[282] This is what our democracy is founded upon.[283] As Westin writes, "[j]ust as a social balance favoring disclosure and surveillance over privacy is a functional necessity for totalitarian systems, so a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies. The democratic society relied on publicity as a control over government, and on privacy as a shield for group and individual life."[284]

To be sure, we need not look far back in the threads of history to find totalitarian governments using sophisticated methods of surveillance as a means of controlling their citizens. Reconsider the Soviet Union, Communist China, Nazi Germany, Fascist Italy, and parts of South Africa that all used overt observation techniques, "interrogation, eavesdropping . . . and other means of data collection to convince their [citizens] that their independent or 'antisocial' thought, speech, and behavior was unacceptable" in modern day society.[285] Often, the threat and implementation of continuous surveillance alone was enough to "keep people in line," but where it was not, the data collected through use of technology was then used to identify and publish dissenters of social norms that the governments deemed dangerous.[286]

Ignazio Silone wrote about the surveillance conditions in the Fascist Italy society in his book *Bread and Wine*.[287] Silone writes, "[i]t is well-known . . . that the police have their informers in every section of every big factory, in every bank, in every big office . . . . This state of affairs spreads suspicion and distrust throughout all classes of population. On this degradation of man into a frightened animal, who quivers with fear and hates his neighbor in his fear, and watches him, betrays him, sells him, and then lives in fear of discovery . . . . The real organization on which the system in this country is based is the secret manipulation of fear."[288]

---

280. McFarland, *supra* note 241.
281. *Id.*
282. *Id.*
283. *Id.*
284. WESTIN, *supra* note 276, at 24.
285. McFarland, *supra* note 241.
286. *Id.*
287. IGNAZIO SILONE, BREAD AND WINE (Signet 2005).
288. *Id.*

Governments today still use surveillance as an "instrument of oppression."[289] In 1996, Phillip Zimmerman, author of *PGP (Pretty Good Privacy)*, wrote about a letter he once received from a human rights activist in Yugoslavia.[290] Zimmerman relays the message by writing, "[o]ur various offices have been raided by various police forces looking for evidence of spying or subversive activities. Our mail has been regularly tampered with and out office in Romania has a constant wiretap. Last year . . . the security police raided our office and confiscated our computers in hopes of retrieving information about the identities of people who complained . . . ."[291] More recently, dissenters on social media and on other Internet sources commenced the "Arab Spring" uprising, a series of government protests that opposed oppressive government regimes and substandard living conditions, which led Egypt and Libya to shut down the internet in an attempt to stifle dissent.[292] Again, as discussed earlier, China and its extreme monitoring has met constant backlash from activist groups due to their censorship of the Internet.[293]

These same tactics hit home when we analyze the tactics used by the National Security Agency ("NSA") and other high ranking offices and officials.[294] From 1952–1974, the NSA and armed forces "kept files on about 75,000 Americans, including civil rights and antiwar activists, and even members of Congress."[295] In the early 1970's, the Nixon Administration broke into the office of the psychiatrist for Daniel Ellsberg, who was suspected of leaking the Pentagon Papers,[296] and stole the psychiatrist's records.[297] Fast forward to the 1996 presidential campaign, which "revealed that the Clinton White House had access to the FBI investigative records of 300 Republications who had served in the Reagan and Bush administrations."[298] What was claimed to be a mistake by the

289. McFarland, *supra* note 241.

290. PHILLIP ZIMMERMAN, *Thanks from Central Europe*: *Letters to Phil from Human Rights Group*, https://philzimmermann.com/EN/letters/index.html (last visited Jan. 25, 2020) [https://perma.cc/RK3L-HMYK].

291. *Id.*

292. McFarland, *supra* note 241; *see also* LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 61–63 (N.Y. Free Press 2011).

293. McFarland, *supra* note 241; *see also* Howard W. French, *Chinese Discuss Plans to Tighten Restrictions on Cyberspace*, N.Y. TIMES (July 4, 2006), https://www.nytimes.com/2006/07/04/world/asia/04internet.html [https://perma.cc/RBQ6-H7RA] .

294. McFarland, *supra* note 241.

295. *Id.*; *see also* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 130–31 (N.Y. Random House 1984).

296. McFarland, *supra* note 241; *see also* BURNHAM, *supra* note 295, at 176.

297. McFarland, *supra* note 241.

298. *Id.*

Clinton administration was termed by the FBI as an "egregious violation of privacy."[299]

More recently, government surveillance increased after the 9/11 terrorist attack, fueling increased power for the NSA.[300] *Wired* magazine described the power of the NSA as, "[e]stablish[ing] listening posts throughout the nation to collect and sift through billions of email messages and phone calls, whether they originate within the country or overseas. It has created a supercomputer of almost unimaginable speed to look for patterns and unscramble codes. Finally, the agency has begun building a place to store all the trillions of words and thoughts and whispers captured in its electronic net."[301]

Privacy is not absolute, and it should not be. Governments do need information, including personal information in order to govern effectively and to protect the security of American citizens; however, American citizens expect and deserve protection from "overzealous and malicious use" of our personal information, especially by governments that have enormous power.[302] Privacy values, rights, and expectations deserve protection against unregulated governmental use of facial recognition technology that compiles an individual's biometric data. To ensure a proper balance, a comprehensive statutory act could provide privacy protections, securing an individual's dignity, personal freedom, and individual qualities, while still properly allowing for compilation of biometric data under appropriate measures and circumstances.

B. Proposed Statutory Act Based on The Wiretap Act

A proposed statutory act that draws heavily from key provisions of the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act")[303] would maintain the ultimate balancing of ensuring individual privacy protections while equally equipping government authorities of all levels with the regulated and controlled use of facial recognition technology. This subsection sets forth in detail below key provisions that the proposed statutory act would take from the Wiretap Act.

There are seven key provisions in particular that the proposed statutory act would implement from the Wiretap Act.[304] Among these

---

299. *Id.*; *see also* Brian McGrory, *FBI Report Condemns File Request*, BOS. GLOBE, June 15, 1996, at 1.

300. McFarland, *supra* note 241.

301. *Id.*; *see also* James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012), https://www.wired.com/2012/03/ff-nsadatacenter/ [https://perma.cc/Q5NP-ZWQ2].

302. McFarland, *supra* note 241.

303. Omnibus Crime Control and Safe Streets Act, 18 U.S.C.A. §§ 2510 *et seq.*

304. *Id.*

provisions is, first, a general prohibition against unregulated use of facial recognition technology that compiles biometric data. Second is a provision allowing for a search warrant based on the Fourth Amendment probable cause standard to allow compilation of biometric data on a certain individual for a specific period of time. Third are restrictions on the application process by allowing only investigators and prosecutors to apply for the search warrant. Fourth is a provision limiting the ordering of the search warrant to be executed by a federal district judge, or a state judge of the same level, and the requisite high standard of proof that must be met prior to granting the search warrant. Fifth is a provision describing the process for executing the search warrant and additionally keeping the judge apprised of how the investigative efforts are proceeding. Sixth is a provision allowing for both criminal and civil penalties against violators of the proposed Act. Seventh, any and all evidence obtained by the result of unlawful compilation of biometric data through use of facial recognition technology is inadmissible in court and thus capable of being suppressed by the aggrieved party. Each provision is addressed in chronological order below.

1. General Prohibition Against Compilation of Biometric Data Through the Use of Facial Recognition Technology

The touchstone of the proposed statutory reform is a general prohibition against the collection and maintenance of a comprehensive database containing an individual's biometric data obtained through use of facial recognition technology. This provision draws heavily from the Wiretap Act which provides, in general, that government interception of wire, oral, or electronic communications by private persons, absent consent, is forbidden and unlawful.[305] Like the Wiretap Act, this proposed statutory act provides that absent valid consent, any evidence obtained of criminal activity is improper and unlawful,[306] unless a valid search warrant was obtained prior to using the investigative technology. The search warrant process and requirements are discussed next.

2. Exception to the General Prohibition: A Search Warrant Based on Probable Cause

Under this proposed statutory act, any government authority may lawfully compile biometric data through the use of facial recognition technology so long as a valid search warrant is obtained prior to using such technology. Like the Wiretap Act, this reform calls for a search warrant that

305. 18 U.S.C.A. § 2511(2)(d).
306. 18 U.S.C.A. § 2511(1)(a)–(e).

complies with standard Fourth Amendment requirements.[307] The probable cause standard under the Wiretap Act requires that the judge make a finding of probable cause that shows "an individual is committing, has committed, or is about to commit a particular offense."[308] The probable cause standard, like the Fourth Amendment standard, requires that the information be specific and particularly describe the place(s) to be searched and the person(s) or thing(s) to be seized.[309]

Along the same lines, the information provided must establish probable cause that compilation of the data will produce images from the facial recognition technology that concerns the particular suspected offense and will be produced from cameras located in specific targeted facilities or premises.[310] By requiring a strict probable cause standard that is sufficiently specific and detailed, legislatures would ensure that law enforcement efforts are tailored to reduce overly broad search efforts and, additionally, are based on reliable and accurate sources of information.

3. The Search Warrant Application Process

In order to curb any potential violations by investigative officials, the proposed statutory reform, like the Wiretap Act, would impose extra constitutional requirements within the search warrant application process. More specifically, the application process would limit potential applicants to federal (or state) investigators and prosecutors that are specifically authorized to apply for a warrant.[311] Where investigators or prosecutors are authorized to apply for a search warrant, the application will be limited to specific crimes.[312] Trivial crimes such as minor offenses or misdemeanors would be outside the purview of the search warrant application and thus could not be applied for.

To address concerns of prosecutors or investigators who take advantage of the search warrant application process (applying very often), this Act, like the Wiretap Act, would require applicants to inform the judge of all known past applications that involve the same persons, facilities, or places.[313] Additionally, past denied or granted applications would have to be reported to the judge.[314]

---

307. 18 U.S.C.A. §§ 2518(3)(b), (d); *see also* Maryland v. Pringle, 540 U.S. 366 (2003); Illinois v. Gates, 462 U.S. 213 (1983) (both cases generally describing the probable cause standard for Fourth Amendment purposes).

308. 18 U.S.C.A. § 2518(3)(a).

309. 18 U.S.C.A. § 2518(4)(a)–(e).

310. 18 U.S.C.A. § 2518(3)(b).

311. 18 U.S.C.A. § 2516(1).

312. § 2516(1).

313. 18 U.S.C.A. § 2518(1)(e).

314. § 2518(1)(e).

Perhaps of greatest importance, the proposed statutory reform would require that an application for the search warrant only be made when prior "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be dangerous."[315] Before the judge will grant the search warrant, she must be satisfied that all requirements have been met and that issuing the search warrant is an investigative measure being taken as a last resort.

4. Limitations on Who May Issue the Order Granting the Search Warrant

Conventional search warrants provide for the issuance of a search warrant by a neutral and detached magistrate.[316] The Wiretap Act calls for higher protections.[317] The proposed statute would only allow a federal district court judge, circuit court judge, or state court judges of similar status to issue a valid search warrant.[318] In reviewing the applications for the search warrant, the judge must be satisfied that all application requirements are met. Even where these requirements are met, the judge, in her official capacity, may still decide to deny the application.[319]

Where the judge does decide to grant the search warrant, she is further empowered with numerous other controls in order to maintain the limited scope of the investigative search. Among these controls includes the requirement that investigators or prosecutors submit to the court periodic reports that discloses the progress that has been made towards the goal of the investigation.[320]

Moreover, the granted search warrant, like traditional search warrants executed pursuant to the Fourth Amendment, must be limited in duration of time throughout the day.[321]

5. Guidelines for Conducting the Search

Once the judge has issued a valid search warrant, the proposed statutory reform requires the investigative officers to use the technology in such a manner that minimizes the interception of captured and stored images that are not the subject of the search warrant.[322] Once the officers have achieved their "authorized objective," all investigative efforts must be

315. 18 U.S.C.A. § 2518(3)(c).

316. *See* Coolidge v. New Hampshire, 403 U.S. 443, 450 (1971).

317. *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, § 1:10 *Title III*, *in* WIRETAPPING & EAVESDROPPING, Westlaw (database updated Nov. 2019).

318. 18 U.S.C.A. § 2510(9)(a).

319. *See* FISHMAN & MCKENNA, *supra* note 317.

320. 18 U.S.C.A. § 2518(6).

321. 18 U.S.C.A. §§ 2518(1)(d), 4(e).

322. 18 U.S.C.A. § 2518(5).

stopped.[323] Where investigative efforts are unsuccessful and do not produce evidence of the suspected crime within the specific timeline allowed by the search warrant, then all efforts must seize.[324] Conduct effectuated by the search is solely limited to use of facial recognition technology, and thus no other investigative efforts may be used pursuant to the search warrant. Once incriminating images are captured, all images must be turned over to the judge who issued the search warrant.[325]

6. Penalties for Violations of the Proposed Statutory Reform

Similar to the Wiretap Act, violators of the proposed statutory reform would be liable for both criminal[326] and civil sanctions.[327] Any aggrieved parties may bring a civil cause of action if their biometric data is wrongfully captured, disclosed, or used by government officials.[328]

7. Suppressing Unlawfully Obtained Evidence

Similar to the Wiretap Act, the proposed statutory reform would allow for any aggrieved person to move to suppress any unlawfully obtained evidence and thus would render such evidence inadmissible in court.[329] Unlawfully obtained evidence may be suppressed where: (1) the biometric data was unlawfully obtained; (2) the order granting the search warrant was insufficient on its face; or (3) the acts that led to the discovery of information from the use of the facial recognition technology did not comply with the scope of the valid search warrant.[330] The motion to suppress may be made at trial, hearings, or proceedings within any court that has jurisdiction.[331]

The aforementioned seven touchstone provisions of the proposed act ultimately seek to implement a comprehensive act that provides law enforcement and the courts with the ability to apply clear standards. The objective of the proposed statutory act is to maintain a much-needed balance between individual privacy protections while still allowing law enforcement access to the valuable tool of facial recognition technology.

Subsection (C), discussed next, explores the strengths and viability of a legislative measure based in large part on the Wiretap Act, while addressing relevant counterarguments.

---

323. § 2518(5).
324. § 2518(5).
325. 18 U.S.C.A. § 2518(8)(d).
326. 18 U.S.C.A. § 2511(1).
327. 18 U.S.C.A. § 2520.
328. 18 U.S.C.A. § 2520(a).
329. 18 U.S.C.A. § 2518(10)(a)(i)–(iii).
330. § 2518(10)(a)(i)–(iii).
331. § 2518(10)(a)(i)–(iii).

C. A Proposed Statutory Act Based on the Wiretap Act Is An Effective Measure to Protect Privacy Interests

The proposed statutory act is an effective measure to protect privacy rights, while also permitting governmental use of facial recognition technology that compiles an individual's biometric data, because the proposed act creates comprehensive guidelines and standards. The suggested provisions in the proposed act provide both judges and law enforcement with clear criteria and requirements in obtaining a warrant that would allow the compilation of an individual's biometric data, under the appropriate circumstances. To be sure, the history of the Wiretap Act demonstrates that its efforts have largely been successful, on the whole, in providing guidelines for judges and law enforcement in granting access to wiretap a suspect's telephone line. Concerns of clarity and uniformity in application of wiretapping laws are further bolstered by the fact that courts repeatedly defer to the Wiretap Act, even where there are gaps in the legislation. Legislatures, additionally, have institutional advantages in creating comprehensive statutory laws to address sophisticated technology. These arguments will be addressed in turn.

1. History Demonstrates that the Wiretap Act is Effective

The practice of wiretapping became commonplace soon after the arrival of the telegraph in 1837 and the invention of the telephone in 1876.[332] Issues soon began to arise when business competitors endeavored to surreptitiously spy in on private conversations for private gain.[333] Catching onto this practice, legislatures began to pass statutes prohibiting wiretapping.[334] California passed the first statute in 1862, and by 1928, more than half of the states had fashioned varying laws outlawing the private practice of wiretapping.[335]

Prior to 1919 and the National Prohibition Act, courts had yet to consider whether law enforcement use of wiretapping violated Fourth Amendment protections.[336] Soon after the passing of the National Prohibition Act, the number of federal criminal cases greatly increased, and the number of executed search warrants exponentially increased.[337] Due to the increase in the unlawful production and transportation of alcohol, the use of wiretapping began to increase throughout the United States. By

332. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 840–41 (2004).

333. *Id.* at 841.

334. *Id.*

335. *Id.*

336. *Id.*

337. Kerr, *supra* note 332, at 842.

1928, the issue of whether the investigative practice violated Fourth Amendment protections reached the Supreme Court in *Olmstead v. United States*.[338] In *Olmstead*, Chief Justice Taft, writing for the Court in a 5–4 decision, held that the practice of wiretapping did not violate the Fourth Amendment because the government did not physically trespass onto Olmstead's property;[339] however, Chief Justice Taft invited Congress to pass statutory protections, allowing for the exclusion of evidence obtained from wiretapping.[340]

Six years after the *Olmstead* opinion, Congress followed through with Chief Justice Taft's suggestion and passed the Communications Act of 1934,[341] which prohibited the disclosure of evidence obtained from wiretapping.[342] The Communications Act clearly made wiretapping a criminal offense, but the specific remedy provided for by the Act remained unclear.[343] Three years after the passing of the Communications Act, the Supreme Court, in *Nardone v. United States*, upheld the validity of the Communications Act and determined that the Act's remedy served as an evidentiary function, rendering all wiretapping evidence inadmissible in federal courts.[344] The importance of *Nardone* was not necessarily the opinion itself but instead the Court's willingness to accept Congress's role in the privacy sphere, by deferring the Court's judgments to the more defined statutory law crafted by Congress, and the Court clarifying gaps in the statutes, such as in *Nardone*, when need be.[345] Notably, in effect, the Communications Act outlawed the practice of wiretapping, inherently overruling the *Olmstead* holding, and the Court raised no issue with this.[346]

Over the course of the next thirty years, wiretapping laws would remain largely unchanged.[347] At this time, thirty-six states have banned wiretapping, but of the thirty-six, twenty-seven states still allow the interception of communications through wiretapping under appropriate circumstances.[348] At the time, the most prominent state wiretapping law was New York's statute, which prohibited wiretapping unless pursuant to a valid search warrant.[349] The constitutionality of the New York statute was

338. *Id.* at 843; *see* Olmstead v. United States, 277 U.S. 438 (1928).

339. *See supra*, Section III(B) for a discussion on the *Jones* test which focuses on property law concepts.

340. *Olmstead*, 277 U.S. at 465–66; Kerr, *supra* note 332, at 845.

341. *See* Communications Act of 1934, 47 U.S.C.A. § 605.

342. Kerr, *supra* note 332, at 845.

343. *Id.*

344. *Id.*; *see* Nardone v. United States, 302 U.S. 379, 384 (1937).

345. Kerr, *supra* note 332, at 846.

346. *Id.*

347. Kerr, *supra* note 332, at 846–47.

348. *Id.* at 846.

349. *Id.*

addressed in 1967 in the case of *Berger v. New York*.[350] *Berger* proved to be an opinion of great significance because the Court's opinion would lay down requirements for future wiretapping laws, consistent with Fourth Amendment principles.[351] The *Berger* requirements include (1) that "a neutral and detached authority" evaluate whether probable cause exists before wiretapping occurs; (2) that the application for the court order to explain "[w]hat specific crime has been or is being committed," "the place to be searched," and "the persons or things to be seized"; (3) that the order authorizing the wiretapping "places a termination date" on the surveillance; (4) that there is "notice as [with] conventional warrants," or "some showing of special facts" to excuse notice; and (5) "a return on the warrant."[352] Since the New York statute did not have many of the requirements, the *Berger* Court held the statute was unconstitutional.[353]

Professor Kerr discusses how *Berger* was abnormal in the sense that the Court reviewed the statute on a facial challenge, as opposed to an as applied challenge to Berger.[354] Kerr suggests that this unusual facial challenge in *Berger* was not mere happenstance but the Court's awareness of Congress's interest in revising the federal wiretapping laws that had proved to be insufficient.[355] This contention is further bolstered by Justice White's dissent in *Berger*, where Justice White noted that Congress, at this point in time, was patiently awaiting the Court's decision to see how the Court would rule, to determine what the *Berger* opinion meant for future wiretapping laws and the requisite provisions needed to comply with Fourth Amendment protections.[356] A plausible suggestion and extension is that the Court recognized, at this time, Congress was best fit to develop a comprehensive plan that would provide guidance to judges and law enforcement. This suggestion is supported by Justice Black's dissent in the *Katz v. United States* opinion.[357] Justice Black, dissenting, discussed the majority's efforts to "guide States in the enactment and enforcement of

350. *Id.* at 847; *see* Berger v. New York, 388 U.S. 41 (1967); *see also* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (the constitutionality of the state statute was capable of being addressed because the Court in *Mapp* held the Fourth Amendment exclusionary rule was now applicable to the states).

351. Kerr, *supra* note 332, at 848.

352. *Id.*

353. *Id.*

354. *Id.* at 847–48.

355. *Id.*

356. *Berger*, 388 U.S. at 112 (White, J., dissenting) ("Bills have been introduced at this session of Congress to fill this legislative gap, and extensive hearings are in progress before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, and before Subcommittee No. 5 of the House Committee on the Judiciary."); *Id.* at 848.

357. Kerr, *supra* note 332, at 849; *see also* Katz v. United States, 389 U.S. 347 (1967).

laws passed to regulate wiretapping by government [in accord with the Fourth Amendment]."[358] The *Berger* and *Katz* decisions demonstrate that the Court carefully rendered its opinion in a carefully timed manner to influence the statutory law that was soon to come.[359]

Two weeks after the *Berger* opinion, Congress proposed the Electronic Surveillance Control Act.[360] Soon thereafter, two more proposals were made to comply with the *Katz* opinion.[361] In 1968, Congress would pass the Wiretap Act, based on *Berger* and *Katz*.[362] The Wiretap Act has been governing law on government use of wiretap since its implementation.[363]

Turning to modern wiretapping law, post *Berger*, *Katz*, and the Wiretap Act, statutory law remains the guiding force in deciding wiretapping cases.[364] Over the course of the past fifty years, Fourth Amendment decisions regulating wiretapping remain rare.[365] As Professor Kerr notes, when courts are confronted with claims that wiretapping violated the Fourth Amendment, courts have deferred back to the Wiretap Act, and its formidable privacy protections, instead of conducting a separate Fourth Amendment analysis or even addressing the law on facial grounds.[366]

To be sure, the Wiretap Act remains the guiding force in deciding wiretapping cases, but the comprehensive Act has its gaps, holes, and weaknesses.[367] In fact, there are many forms of new technologies, like video surveillance, GPS monitoring, and satellite technology that Congress has wholly left unregulated.[368] But what remains compelling about the Wiretap Act is that, with even areas of weakness, courts remain reluctant to find these holes in violation of the Fourth Amendment, and instead, the courts have continued to defer to Congress and the protections it has afforded.[369] For example, the Sixth Circuit, in *McKamey v. Roach*,[370] considered the constitutionality of the practice of wiretapping of cordless phone calls, which was specifically exempted by the Wiretap Act. Yet even in *McKamey*, the Sixth Circuit refused to rule that the Fourth Amendment

358. *Katz*, 389 U.S. at 364 (Black, J., dissenting).
359. Kerr, *supra* note 332, at 849–50.
360. *Id.* at 850.
361. *Id.*
362. *Id.*
363. *Id.*
364. *Id.*
365. *Id.*
366. *Id.* at 850–51.
367. Daniel Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call For Judicial Deference*, 74 FORDHAM L. REV. 747, 763 (2005).
368. *Id.*
369. Kerr, *supra* note 332, at 852.
370. McKamey v. Roach, 55 F.3d 1236, 1238 (6th Cir. 1995).

provided protection from warrantless wiretapping of cordless phone calls, otherwise decisively left unprotected by the Wiretap Act, and instead, the Sixth Circuit deferred to Congress, and the protections afforded by the Wiretap Act.[371] The same year *McKamey* was decided, the Fourth Circuit, in *United States v. McNulty*, a case also involving warrantless wiretapping of cordless phone calls, stated:

> In the fast-developing area of communications technology, courts should be cautious not to wield the amorphous "reasonable expectation of privacy" standard, in a manner that nullifies the balance between privacy rights and law enforcement needs struck by Congress in Title III . . . . As new technologies continue to appear . . . the primary job of evaluating their impact on privacy rights and of updating the law must remain with the branch of government designed to make such policy choices, the legislature.[372]

Litigants have further challenged the Wiretap Act, and its gaps, when arguing for potential civil claims under the Fourth Amendment for illegal wiretapping.[373] The Sixth Circuit, in *Adams v. Battle Creek*, deferred to the Wiretap Act, holding that the only appropriate remedy for illegal wiretapping practices are statutory claims that are provided under the Wiretap Act.[374] In other words, the *Adams* court deferred to the Wiretap Act protections and refused to further extend Fourth Amendment protections by otherwise allowing for civil remedies under the Constitution.[375] The *Adams* court reached this holding because the Wiretap Act "seeks to balance privacy rights and law enforcement needs, keeping in mind the protections of the Fourth Amendment against unreasonable search and seizure."[376]

Deference has further been conferred to Congress and Title III in cases involving covert video surveillance, which is specifically exempted from the Wiretap Act.[377] In reviewing this gap in the Wiretap Act, courts have held that Fourth Amendment protections are satisfied so long as the government complies with equivalent statutory standards set forth in the Wiretap Act which regulate audio wiretapping.[378] In other areas that Congress's Wiretap Act has left unregulated, courts, rather than crafting new constitutional law rules, defer to adopting the nearest statutory

371. *Id.* at 1239–40.
372. *See* United States v. McNulty, 47 F.3d 100, 104–06 (4th Cir. 1995).
373. Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001).
374. *Id.*
375. Kerr, *supra* note 332, at 853; *see also Adams*, 250 F. 3d at 986.
376. Kerr, *supra* note 332, at 853; *see also Adams*, 250 F. 3d at 986.
377. Kerr, *supra* note 332, at 854; *see also Adams*, 250 F.3d at 986.
378. Kerr, *supra* note 332, at 854; *see also Adams*, 250 F.3d at 986.

requirements.[379] Remarkably, in national security cases involving wiretapping, the Supreme Court even went as far as calling on Congress to enact new standards to address national security contexts under the Wiretap Act, rather than taking its own measures to craft new Fourth Amendment case law to address these issues.[380]

The above efforts are made to demonstrate three points: (1) the proposed statutory act, based on the Wiretap Act, is likely constitutional; (2) courts, in areas of sophisticated technology, defer to Congress; and (3) continued deference by courts, over the course of the past fifty years, allows for clarity and uniformity in application.

To be certain that the proposed act is likely constitutional, recall from the discussion above, the Wiretap Act was fashioned and manufactured based off of the requirements laid down by the Court in *Berger* and *Katz*. These efforts, reliant upon *Berger* and *Katz*, were taken by Congress to ensure further wiretap statutes would comply with Fourth Amendment protections. Once the Wiretap Act was drafted and enacted, it has survived numerous facial challenges over the course of fifty years and remains standing as the controlling wiretap statute. What does this mean for a proposed act regulating facial recognition technology, that is based on the Wiretap Act? We can be sure that the key provisions in the proposed act would likely be held to be constitutional, in accord with Fourth Amendment protections since these key provisions have repeatedly been held to be constitutional.

Based on the history of the Wiretap Act, a proposed act regulating governmental use of facial recognition technology would likely be deferred to by the judicial branch, even if there were gaps and holes in the proposed act. To be sure, the Wiretap Act, like any other statute, does have its weaknesses. However, these same gaps and holes may either be inapplicable to the proposed act or could otherwise be remedied upon drafting and enactment of the proposed act. In other words, this is the perfect opportunity for Congress to learn from past mistakes in implementing reform to regulate governmental use of facial recognition technology.

Opposers to statutory protections may doubt the ability of Congress to draft a comprehensive act that provides detailed guidance for every single situation. Yet, even if a proposed act were to result in gaps, the history of the Wiretap Act demonstrates that a proposed act would be deferred to by the various court systems. This deference ultimately provides for clarity and uniformity of law; law enforcement agencies and judges can be sure that law enforcement actions comply with both Fourth Amendment protections, and statutory protections, when the statutory act is complied

379. Kerr, *supra* note 332, at 854; *see also Adams*, 250 F.3d at 986.

380. Kerr, *supra* note 332, at 854; *see also* United States v. United States District Court, 407 U.S. 297, 322–23 (1972); *Adams*, 250 F.3d at 986.

with. Stated another way, so long as law enforcement complies with the detailed mandates of the proposed act, the actions are constitutional. If the proposed act does result in gaps in protection, courts will likely still defer to the proposed act, which provides the opportunity for Congress to amend a small portion of the proposed statutory act, otherwise not resulting in large change in application of the law.

Furthermore, Legislatures have institutional advantages to craft effective comprehensive statutory acts to balance privacy rights and government needs. This argument is addressed next.

2. Legislatures Have Institutional Advantages to Create Effective Comprehensive Statutory Law that Balances Privacy Rights and Government Needs

Legislatures have distinct institutional advantages that provide for the ability to draft and implement detailed comprehensive statutory reform.[381] Because of these advantages, legislatures are capable of creating rules that address quickly changing and complex technologies. Among these advantages include (1) the ability to create rules ex ante (for the future); (2) flexibility in drafting and amending laws; and (3) the power to draft rules tailored to a wide range of inputs from competing views.[382] Each advantage will be addressed more in depth below.

a. Crafting Rules for the Future

First, Congress and state legislatures have the distinct power to draft laws ex ante, or for the future.[383] With this advantage, legislatures are capable of acting at any time, even when technology is new.[384] This allows for legislatures to combat newly changing technologies by acting early in the development or implementation of the technology.[385] History corroborates this point. Consider the Electronic Communications Privacy Act which regulates the privacy of emails.[386] This Act was implemented in 1986, before most Americans used the technology for commercial or personal uses.[387]

To appreciate this advantage, the court system and its disadvantages must be considered. Courts, as opposed to legislatures, cannot enact comprehensive rules of law in an expedited manner.[388] Instead,

381. Kerr, *supra* note 332, at 867.
382. *Id.* at 867–82.
383. *Id.* at 868.
384. *Id.*
385. *Id.* at 870.
386. *Id.*
387. *Id.*
388. *Id.* at 868–69.

courts must first wait for the appropriate case to make its way into the court system.[389] Before the appropriate case can come to fruition, the specific technology at issue must first be used by government officers in the course of investigating a criminal offense.[390] Such technology must then produce evidence of a crime, and from there the defendant must raise a constitutional challenge on the use of the technology.[391] After the long process of the initial trial, there may be an appeal.[392] However, many, if not most, defendants enter into a plea deal.[393] If the defendant does not enter into a plea deal, then he likely waives his right to an appeal.[394] If this is the case, an appellate decision is unlikely and will only arise in rare cases.[395] From there, the appellate decision must be published to become a precedential decision.[396] At that point, if the defendant appeals, the Supreme Court may not even take the case, and if it does, a decision will not be rendered until years after the circuit courts have addressed the issue.[397]

This ultimately leads to judicial rulemaking on the basis of now outdated technology and outdated factual records. In a state of current changing technology and the use of facial recognition technology that subjects American citizens to violations of privacy, comprehensive and detailed legislative rules that project for future violations are needed to ensure expectations of privacy.

b. Flexibility

The second institutional advantage of legislative rules is that legislatures have the capability of enacting rules quickly and additionally hold the derivative advantage of amending rules quickly.[398] This advantage allows for legislatures to ensure the balance of privacy rights against law enforcement needs for the investigative technology with newly arising circumstances and variations of technology.

Technology and the use of new and varying forms of technology requires governing bodies to act quickly to ensure privacy protections.[399] But, in order to ensure the intended balance among privacy rights and law enforcement needs to combat crimes, legislatures have mechanisms to keep

389. *Id.*
390. *Id.*
391. *Id.* at 868.
392. *Id.*
393. *Id.*
394. *Id.*
395. *Id.*
396. *Id.*
397. *Id.*
398. *Id.* at 871.
399. *Id.*

up with technological change.[400] Legislatures are capable of experimenting with different rules and have the ability to make frequent amendments to the law.[401] For example, the ECPA enacted in 1986 amended the Wiretap Act.[402] The ECPA itself has been further amended eleven separate times.[403] While some amendments brought about large change and others smaller technical amendments, the same goal was maintained: balancing privacy interests and government's need to stop crime.[404]

It should be noted that this argument is criticized by some privacy scholars, most notably Professor Solove.[405] Professor Solove argues that judicial rules can be just as flexible, comprehensive, and detailed as legislative rules.[406] Solove argues that judicial rules under the Fourth Amendment are balanced and detailed because, once the Court finds an action deserves protection, the Court lays down specific rules to regulate the particular search and seizure.[407] The balance struck between privacy rights and law enforcement needs is accomplished through the warrant requirement of the Fourth Amendment.[408] Professor Solove goes further to suggest that in situations where warrants do not work well, the Court has crafted specific exceptions to the warrant requirement, such as with Terry stops, "special needs," and exigent circumstances.[409]

Professor Solove's arguments are compelling in some Fourth Amendment situations, but his arguments lose support in the context of governmental use of facial recognition technology. At the outset, the proposed statutory act that regulates governmental use of facial recognition technology is far more detailed than simply requiring a standard warrant supported by probable cause. Instead, the proposed statutory act provides other requirements, such as requiring periodic reports to an overseeing judge about law enforcement efforts in conducting the surveillance. It is the other requirements, in addition to the warrant provision, that ensure the balance among privacy rights and law enforcement needs. It is true that, in theory, the Court *could* craft a verbose and detailed opinion that laid out every single specific guideline for governmental use of facial recognition technology, but is the Court prepared to do so? For one, American citizens and law enforcement would be required to wait around until the perfect case finally arose to the Supreme Court, and only then, the Court would still have to go out of its way to draft comprehensive guidelines for addressing

400. *Id.*
401. *Id.*
402. *Id.*
403. *Id.*
404. *Id.* at 871–72.
405. Solove, *supra* note 367, at 762.
406. *Id.*
407. *Id.* at 761–62.
408. *Id.* at 762.
409. *Id.*

governmental use of facial recognition technology. This will take years, at best, leaving privacy rights in limbo.

Governmental use of facial recognition technology, moreover, is dissimilar to the exceptions to the warrant requirement that are argued by Professor Solove. In other words, governmental use of facial recognition technology is a circumstance where a warrant *must* be required, not like exigent circumstances or "special needs," where either the lesser standard of reasonable suspicion or no warrant at all are required. This is certain because the Supreme Court, for over the course of fifty years, has maintained that generally a warrant is required to wiretap a suspect's telephone. If a warrant is required to wiretap a person's telephone, there can be no doubt then that a warrant should be required to compile a comprehensive database of an individual's biometric data, effectively establishing the person's location and actions for every second of every day.

Another lingering issue with judicial rules is that courts are strongly limited by stare decisis.[410] With technology constantly changing and growing in its capabilities, legislatures are the appropriate governing body for drafting comprehensive statutory law to protect American citizens against unregulated facial recognition technology use.

c. Legislative Information Surplus

Third, legislatures have the advantage of crafting legislative rules based on a wide range of input provided from parties arguing differing opinions that allows legislatures to create the most well-balanced rules.[411] Legislative rules tend to be crafted from inputs and information taken from legislature hearings, poll results, advocacy by interest groups, and other arenas.[412] With the case at hand, drafting a well-balanced and intricate set of rules requires a comprehensive understanding of the underlying technological facts.[413] Legislatures have the ability to receive and discuss this information due to the wide range of inputs.[414] Courts, on the other hand, are limited to a brief factual record, narrow arguments, and short oral arguments.[415]

These three institutional advantages allow for the legislature to create a well-balanced and nuanced rule that is capable of accounting for a variety of information, differing views, and is capable of being amended if need be. These advantages ensure the proper balance between privacy rights against law enforcement needs.

---

410. Kerr, *supra* note 332, at 871.
411. *Id.* at 875.
412. *Id.*
413. *Id.*
414. *Id.*
415. *Id.*

CONCLUSION

As sophisticated technology continues to advance, and as time carries on, unregulated governmental use of facial recognition technology will continue to invade the secrecies of our daily lives, creating an all-encompassing picture of our movement, actions, and relationships. This note has strived to raise awareness to these issues, while putting a face to current law enforcement practices both nationally and internationally. At a minimum, such unregulated use of facial recognition technology is an unreasonable search within the meaning of the Fourth Amendment, and American citizens deserve protection. But an appropriate factual case raising this issue is at best, years away, and it is unknown as to whether the Court would be prepared to lay down comprehensive guidelines for regulated governmental use of facial recognition technology. This note has sought to explain how a comprehensive statutory act, founded upon key provisions of the Wiretap Act, would provide clear guidelines and standards for judges and law enforcement officers. The proposed act would additionally establish a much-needed balance between privacy rights and law enforcement needs. Above all, one thing remains certain: the time to act is now, Congress.