Biometrics and an AI Bill of Rights

*Margaret Hu**

ABSTRACT 283
INTRODUCTION 284
I. FEDERAL GOVERNMENT USE OF BIOMETRIC DATA 286
A. *Biometric Data: Public Collection and Use* 286
B. *DHS Expansion of Biometric Collection* 288
II. BIOMETRICS AND AI 289
A. *High-Risk AI Biometric Systems* 289
B. *Biometric AI Systems and Criminal Procedure Risks* 291
III. AI BILL OF RIGHTS 296
A. *Bill of Rights and Anticipating Biometric AI Harms* 296
B. *Looking Ahead* 297
CONCLUSION 300

ABSTRACT

This Article contends that an informed discussion on an AI Bill of Rights requires grappling with biometric data collection and its integration into emerging AI systems. Biometric AI systems serve a wide range of governmental purposes, including policing, border security and immigration enforcement, and biometric cyberintelligence and biometric-enabled warfare. These systems are increasingly categorized as "high-risk" when deployed in ways that may impact fundamental constitutional rights and human rights. There is growing recognition that high-risk biometric AI systems, such as facial recognition identification, can pose unprecedented challenges to criminal procedure rights. This Article concludes that a failure to recognize these challenges will lead to an underappreciation of

* Professor of Law and International Affairs, Penn State Law and School of International Affairs; Institute for Computational and Data Sciences; The Pennsylvania State University – University Park. The author is grateful for this opportunity to participate in the Duquesne Law Review 2022 Symposium, The Death of Eyewitness Testimony & the Rise of Machine Evidence. Many thanks to Davi Liang and Ashleigh Herrin for their editorial assistance, and to Robert Diehl and Alexis Thurston of the Duquesne Law Review for their editorial leadership.

the constitutional threats posed by emerging biometric AI systems and the need for an AI Bill of Rights.

INTRODUCTION

On October 8, 2021, the White House Office of Science and Technology Policy ("OSTP") invited the public to discuss *Public and Private Sector Uses of Biometric Technologies* through a Notice of Request for Information ("RFI"), published in the Federal Register.[1] Shortly thereafter, OSTP Director Eric Lander and OSTP Deputy Director for Science and Society Alondra Nelson, issued several media and White House releases, including an opinion piece titled, *Americans Need a Bill of Rights for an AI-Powered World*,[2] and a Press Release titled, *Join the Effort to Create a Bill of Rights for an Automated Society*.[3] This Article addresses both: concerns attached to biometric technologies and the need for an AI Bill of Rights.[4]

Rather than treat these topics as separate and distinct, this Article attempts to integrate the two. It argues that biometric AI systems must be seen as a constitutive force behind conceptualizing an AI Bill of Rights. To ground potential AI-driven harms concretely, this Article focuses on facial recognition technology, a biometric technology that utilizes AI. The increasing reliance on facial recognition technology by the government poses unique challenges to

1. Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56,300 (Oct. 8, 2021).

2. Eric Lander & Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, WIRED (Oct. 8, 2021), https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/ (citing, *e.g.*, Drew Harwell, *The Accent Gap*, WASH. POST (July 19, 2018) https://www.washingtonpost.com/graphics/2018/business/alexa-does-not-understand-your-accent/; Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Paul Mozur, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. TIMES (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Tom Simonite, *How an Algorithm Blocked Kidney Transplants to Black Patients*, WIRED (Oct. 26, 2020), https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/).

3. Press Release, White House, Join the Effort to Create a Bill of Rights for an Automated Society (Nov. 10, 2021), https://www.whitehouse.gov/ostp/news-updates/2021/11/10/join-the-effort-to-create-a-bill-of-rights-for-an-automated-society/.

4. Multiple scholars have offered careful analysis of data-driven and algorithmic harms of big data and AI technologies. *See generally, e.g.*, CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016); VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018); SAFIYA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016); Anupam Chander, *The Racist Algorithm?*, 115 MICH. L. REV. 1023 (2017) (book review); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014); Jessica M. Eaglin, *Constructing Recidivism Risk*, 67 EMORY L.J. 59 (2017).

criminal procedure protections under the Bill of Rights. These challenges include potential stressors placed on the Fourth Amendment's protections against unreasonable searches and seizures, the Fifth Amendment's protection of the right against self-incrimination, and the Sixth Amendment's protection to confront witnesses under the Confrontation Clause.[5] Under the Sixth Amendment, for example, a criminal defendant is owed the opportunity to confront witnesses and prosecutorial evidence. However, as this Article explores, confronting AI technologies, such as facial recognition technology that may be presented in a criminal case to establish the defendant's identity or to support evidentiary claims of criminal wrongdoing, may be difficult.[6]

Part I provides an overview of biometric data, including how it is currently defined by the U.S. Department of Homeland Security ("DHS"). It focuses on capture of biometric data by DHS for purposes of border security and homeland security. As a case study, this Article contends that biometric collection by the DHS is indicative of both the government's exponentially increasing appetite for biometric data and the expansion of biometric AI systems. Part II explains why biometric data is increasingly integrated into AI technologies, especially for law enforcement, and intelligence and national security purposes. Part III discusses why an informed effort to create an AI Bill of Rights requires grappling with biometric data and its integration into emerging AI systems, especially for predictive policing and biometric cybersurveillance purposes.

Biometric AI systems are increasingly categorized as "high-risk AI systems" by other governing bodies, such as the European Commission[7] ("EU Commission") and human rights organizations within the European Union ("EU").[8] The EU has recognized that

---

5. U.S. CONST. amends. IV–VI. *See infra* Part II.B. *See also, e.g.*, Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. 1105, 1126 (2021); Eldar Haber, *Racial Recognition*, 43 CARDOZO L. REV. 71, 101 n.165 (2021) (citing State v. Loomis, 881 N.W.2d 749 (Wis. 2016)); Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, N.Y. TIMES (May 1, 2017), https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html); Andrea Roth, *Machine Testimony*, 126 YALE L. J. 1972, 1983 (2017); Joseph Clarke Celentino, Note, *Face-to-Face with Facial Recognition Evidence: Admissibility Under the Post-Crawford Confrontation Clause*, 114 MICH. L. REV. 1317, 1318 (2016).

6. *See infra* Part II.B (citing, *inter alia*, Roth, *supra* note 5).

7. European Commission, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021) [hereinafter EU 2021 Artificial Intelligence Act Proposal].

8. European Digital Rights et al., *A Civil Society Statement: An EU Artificial Intelligence Act for Fundamental Rights*, ALGORITHM WATCH (Nov. 30, 2021), https://algorithmwatch.org/en/eu-artificial-intelligence-act-for-fundamental-rights/.

certain biometric AI systems should be understood as high-risk when impacting fundamental constitutional rights and human rights. In a recent proposal for greater AI regulation, the EU Commission recognized that biometric AI systems require additional oversight and recognition of their potential impact on fundamental rights.[9] This Article concludes that a conversation on an AI Bill of Rights should be paired with a comparative approach to biometric data and biometric AI system regulation that is occurring in the EU. By monitoring the EU's approach to high-risk AI systems generally, and high-risk biometric AI systems specifically, the dialogue on an AI Bill of Rights and AI regulation will be more informed in the United States.

I. FEDERAL GOVERNMENT USE OF BIOMETRIC DATA

A. *Biometric Data: Public Collection and Use*

Biometric identification involves the measurement of physiological characteristics. Biometric data used in biometric identification technologies can include a range of biometric identifiers.[10] In addition to digital photos and video feeds utilized for facial feature analysis through facial recognition technology, other biometric data may include digitally scanned fingerprints and iris scans, keystroke analysis, voice and gait analysis, and other identifiers.[11] DNA is included as a biometric identifier in some contexts and excluded in others.[12] The DHS deemphasizes the genome as a biometric to enable the use of de-identified health data for research purposes, while the DHS includes DNA within a proposed definition of

9. *See infra* Part II.A (citing EU 2021 Artificial Intelligence Act Proposal, *supra* note 7).

10. *See, e.g.*, Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1477 n.3 (2013) (citing, *e.g.*, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES (Joseph N. Pato & Lynette I. Millett eds., 2010); A. MICHAEL FROOMKIN & JONATHAN WEINBERG, CHIEF JUSTICE EARL WARREN INST. ON LAW & SOC. POL'Y, HARD TO BELIEVE: THE HIGH COST OF A BIOMETRIC IDENTITY CARD (2012), http://www.law.berkeley.edu/files/Believe_Report_Final.pdf; KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE (2011); ANIL K. JAIN ET AL., INTRODUCTION TO BIOMETRICS (2011); JENNIFER LYNCH, FROM FINGERPRINTS TO DNA: BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND (2012); SHOSHANA AMIELLE MAGNET, WHEN BIOMETRICS FAIL: GENDER, RACE, AND THE TECHNOLOGY OF IDENTITY (2011); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012)).

11. *See, e.g.*, Margaret Hu, *Biometric Surveillance and Big Data Governance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 121, 126 (David Gray & Stephen E. Henderson eds., 2017).

12. Jennifer K. Wagner et al., Comment Letter on Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies 7 (Jan. 5, 2022) (copy on file with author).

biometrics in order to enable a broad definition for border security and other security rationales.[13] From a governmental standpoint, DNA collection for databasing and database screening by various federal agencies is not clearly defined as biometric *per se*.[14]

The United States federal government is at the earliest stages of regulating how the government should collect and use biometric data. Congress has not clearly defined biometric data or when it is appropriately collected.[15] Federal agencies have commenced the process of attempting to define biometric data under a regulatory regime.[16] As of yet, there is not a unified federal approach to imposing limitations on biometric data collection and use.[17] Experts have noted that there is a need to expressly recognize tensions in how best to define and apply biometric data. Unresolved questions include who is responsible for oversight of biometric standards and the deployment of emerging biometric technologies; how biometric data can be used, by whom, and under what circumstances; and, when biometric systems may be appropriately used for identification purposes or other policy objectives.

Similarly, AI is also at the earliest stages of regulation in the United States. What is not clearly understood by many policymakers in the United States is how certain AI systems are increasingly reliant on biometric data, including the failure to recognize the precise relationships between biometric technology and the AI systems utilized by that technology.[18] Consequently, this Article focuses on how biometric-based AI systems challenge the current data governance frameworks in unprecedented ways[19] that underscore the

---

13. *Id.*

14. *See* Wagner et al., *supra* note 12.

15. *See id.* at 7.

16. *See id.*; *see generally* Dan Berger et al., *Biometric Data and Midnight Regulations*, REGULATORY REV. (Mar. 11, 2021), https://www.theregreview.org/2021/03/11/berger-hu-katsanis-wagner-biometric-data-midnight-regulations/.

17. *See* Wagner et al., *supra* note 12, at 7; *see generally* Berger et al., *supra* note 16. *See also infra* Part III.B.

18. *See, e.g.*, Jan Czarnocki, *Will New Definitions of Emotion Recognition and Biometric Data Hamper the Objectives of the Proposed AI Act?*, *in* 2021 INTERNATIONAL CONFERENCE OF THE BIOMETRICS SPECIAL INTEREST GROUP (BIOSIG) (Arslan Brömme et al., eds., Inst. of Elec'l. & Elec's. Eng'rs 2021); Mia Hoffmann & Mario Mariniello, *Biometric Technologies at Work: A Proposed Use-Based Taxonomy*, POL'Y CONTRIBUTION no. 23, Nov. 2021 (defining "biometric technologies as AI technologies that rely on biometric data to derive inferences about the individual whose data is collected").

19. This Article is a continuation of the author's past research on the legal challenges attached to biometric cybersurveillance. *See* Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633 (2017); Margaret Hu, *Biometric ID Cybersurveillance*, *supra* note 10; Margaret Hu, *Crimmigration-Counterterrorism*, 2017 WIS. L. REV. 955 (2017); Margaret Hu, *Horizontal Cybersurveillance Through Sentiment Analysis*, 26 WM. & MARY BILL RTS. J. 361 (2017); Wagner et al., *supra* note 12.

urgent need for an AI Bill of Rights. The underdevelopment of AI regulation is especially pronounced when examining the risks to criminal defendants and the criminal procedure protections that may be compromised under the Fourth, Fifth, and Sixth Amendments.[20]

B. DHS Expansion of Biometric Collection

To better understand biometric-based AI systems, this Article uses as a case study a DHS-issued Notice of Proposed Rulemaking ("NPRM"), titled *Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (USCIS).*[21] At the end of the Trump administration, on September 11, 2020, a proposed rulemaking illustrated the rapid expansion of proposed biometric data collection, purportedly for the purposes of homeland security and immigration enforcement. Specifically, the NPRM stated that: "Biometrics means the measurable biological (anatomical and physiological) or behavioral characteristics of an individual, including an individual's fingerprints, palm prints, photograph (facial image), signature, iris (iris image), voice (voice print), and/or DNA (partial DNA profile) (subject to the limitations in 8 CFR 103.16(d)(2))."[22] DHS further stated that its biometrics can include "voluntary DNA testing to verify a claimed genetic relationship."[23] The proposed regulation did not rely upon congressional authority. The expansion of both how biometric data was defined as well as how biometric data could be used was dramatic. The NPRM expanded the definition and collection of biometric data to authorize vetting and tracking individuals throughout the "immigration lifecycle." Although the status of the NPRM and biometric collection policy under the Biden administration is unclear, a recent DHS Privacy Impact Assessment ("PIA")[24] appears to adopt DNA verification screening by DHS without clear statutory authority.[25]

---

20. *See infra* Part II.B.

21. Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56,338 (proposed Sept. 11, 2020).

22. *Id.* at 56,414 (emphasis removed).

23. *Id.* at 56,350.

24. DEP'T OF HOMELAND SEC., DHS REFERENCE NO. DHS/CBP/PIA-071, PRIVACY IMPACT ASSESSMENT FOR THE OPERATIONAL USE OF FAMILIAL DNA (2021), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp071-operationaluseoffamilialdna-september2021.pdf.

25. *Id.* at 1 (citing Ms. L. v. U.S. Immigr. & Customs Enf't, 415 F. Supp. 3d 980, 990 (S.D. Cal. 2020) (requiring U.S. Immigration and Customs Enforcement to conduct DNA testing to verify parentage before separating migrant adult from child)); *see also* Tally Kritzman-Amir, *Swab Before You Enter: DNA Collection and Immigration Control*, 56 HARV. C.R.-C.L. L. REV. 77, 78 (2021).

This NPRM illustrates how biometric data forms the cornerstone datapoint for a wide range of AI-driven immigration-related vetting and database screening protocols.[26] DHS often commences screening protocols with biometric data as a form of identity verification. Beyond identity verification, biometric AI tools and systems can assist DHS and other governmental entities with profiling individuals to form the basis of risk assessments and predictive analytics.[27]

The data architecture necessary for biometric AI systems has expanded dramatically in the past two decades since the terrorist attacks of September 11, 2001. There have been proposals for biometric electronic identity cards such as a biometric ePassport,[28] for example, which, if implemented, would dramatically expand biometric data collection through mass collection and universal databasing. Further, the Trump administration's Executive Order 13780, commonly referred to as the Muslim Ban or Travel Ban, mandated the "Expedited Completion of the Biometric Entry-Exit Tracking System" by DHS.[29] The extreme vetting protocols proposed by the Trump administration also expanded social media surveillance as a part of screening procedures.[30] Through biometric AI systems promulgated under predictive policing and national security objectives, biometric cybersurveillance tools fuse biometric and biographic data with social media profiling to assess risk.[31]

II. BIOMETRICS AND AI

A. *High-Risk AI Biometric Systems*

In April 2021, the EU Commission proposed for public comment a comprehensive AI regulation.[32] It explained that the goals of the proposed law were multifold: to safeguard fundamental rights, to ensure a harmonization of EU rules relating to AI, and to promote excellence and trustworthiness in AI and AI regulation.[33] Referred to as the AI Act, the proposal is officially titled: "Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act)

---

26. Hu, *Algorithmic Jim Crow*, *supra* note 19, at 639–40 (internal citations omitted).
27. *See, e.g.*, *id.*
28. *Id.*
29. *Id.* at 640 n.45 (citing Exec. Order No. 13,780, 82 Fed. Reg. 13,209 (Mar. 6, 2017)).
30. *See id.* at 640–41.
31. *See, e.g.*, Margaret Hu, *The Ironic Privacy Act,* 96 WASH. U. L. REV. 1267, 1288–90 (2019).
32. EU 2021 Artificial Intelligence Act Proposal, *supra* note 7.
33. *Id. See also, e.g.*, Mauritz Kop, *EU Artificial Intelligence Act: The European Approach to AI*, TRANSATL. ANTITRUST & IPR DEVS. (Oct. 1, 2021), https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/.

and Amending Certain Union Legislative Acts."[34] The AI Act proposes to adopt a risk-based approach to AI regulation. Article 13, for instance, emphasizes the need for AI transparency: "High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately."[35]

Importantly for the purposes of this Article, the AI Act recognizes the link between AI technologies and biometric identification, and the risk to fundamental rights. The AI Act identifies certain "high-risk AI" technologies that integrate biometric data in contexts that might impose harm in public safety and surveillance.[36] These "high-risk AI systems" are contained in Annex III of the AI Act.[37] Other AI systems are characterized as posing "unacceptable risk."[38] Except for certain law enforcement and national security justifications, the AI Act classifies AI systems that are deployed for real-time biometric identification as falling within the unacceptable risk category.[39]

The AI Act proposes that specific fundamental rights warrant protection from AI harms, such as anti-discrimination values and expressive freedoms. The AI Act identifies that social scoring systems, in particular, "may lead to discriminatory outcomes and the exclusion of certain groups."[40] Specifically, such scoring systems "may violate the right to dignity and non-discrimination and the values of equality and justice."[41] Regarding biometric identification systems, the proposed EU law identifies the intrusive nature of biometric surveillance as infringing upon fundamental freedoms, impacting privacy rights that could lead to "a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights."[42] The proposed AI Act further identifies that criminal procedure protections might be vulnerable to remote biometric identification technologies. The harms associated with biometric AI systems could encompass, for example, databasing, inadequate safeguards, lack of proportionality, probabilistic and predictive consequences, and negative inferences.[43]

---

34. *Id.*
35. EU 2021 Artificial Intelligence Act Proposal, *supra* note 7, at art. 13.
36. Khari Johnson, *The Fight to Define When AI is 'High Risk'*, WIRED (Sept. 1, 2021, 8:00 AM), https://www.wired.com/story/fight-to-define-when-ai-is-high-risk/.
37. EU 2021 Artificial Intelligence Act Proposal, *supra* note 7, at art. 6(2).
38. *Id.* at art. 5, mem. § 5.2.2.
39. *Id.* at art. 5.
40. *Id.* at recital (17).
41. *Id.*
42. *Id.* at recital (18).
43. *Id.* at recitals (19)–(20).

Standalone AI systems identified in Chapter 1 of Title III of the AI Act "with mainly fundamental rights implications that are explicitly listed in Annex III" are AI systems "whose risks have already materialised or are likely to materialise in the near future."[44] For the Annex III high-risk AI systems, the AI Act proposes newly developed AI compliance and oversight mechanisms, including impact assessment procedures.[45] The proposal recognizes the special risks posed by "remote biometric identification systems."[46] The AI Act suggests that internal controls can be implemented by AI providers; however, remote biometric identification systems "would be subject to third-party conformity assessment[,]" and would also be subject to "comprehensive ex-ante conformity assessment through internal checks, combined with a strong ex-post enforcement[.]"[47] Title IV of the law focuses on the manipulative risks of AI systems that involve human interactions and "are used to detect emotions or determine association with (social) categories based on biometric data" or "generate or manipulate content" (such as with deep fakes).[48]

B. Biometric AI Systems and Criminal Procedure Risks

In the United States, biometric AI systems place unique stress points on criminal procedure protections, demonstrating why they are fairly characterized as "high-risk."[49] AI is increasingly integrated into criminal investigation and used as evidence.[50] There are several points in a criminal investigation and proceeding where biometric AI and cybersurveillance are vulnerable to failing to

---

44. *Id.* at mem. § 5.2.3.
45. *Id.* at tit. III, chs. 2, 3.
46. *Id.* at recital (18).
47. *Id.* at mem. § 5.2.3.
48. *Id.* at mem. § 5.2.4.
49. *See generally, e.g.*, ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING (2017); Jennifer Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Non-Custodial Prevention*, 99 CORNELL L. REV. 327 (2014); Kelly Hannah-Moffat, *Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates*, 23 THEORETICAL CRIMINOLOGY 453 (2019); Margaret Hu, *Algorithmic Jim Crow*, *supra* note 19; Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043 (2019); Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. 192 (2019); Sahil Chinoy, Opinion, *The Racist History Behind Facial Recognition*, N.Y. TIMES (July 10, 2019), https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html; Woodrow Hartzog & Evan Selinger, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66/.
50. Christopher Rigano, *Using Artificial Intelligence to Address Criminal Justice Needs*, NAT'L INST. JUST. (Oct. 8, 2018), https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs.

conform to the protections historically afforded under the Fourth, Fifth, and Sixth Amendments.

Under the Fourth Amendment, biometric AI concerns encompass the collection, use, and storage of biometric data. The presentation of biometric data—for example, the public view of one's face, either physically or digitally—can be captured in a digital image and then processed by facial recognition technology. If the government undertakes the collection of facial images, it could be argued that this falls outside the scope of a search and seizure. This is especially true if the biometric data collection was collected administratively and not in the service of a specific law enforcement investigation. Therefore, broad surveillance captures may fall outside of the warrant requirement of the Fourth Amendment.[51]

In AI systems, biometric data collection and use often does not stop with a simple data point, such as a digital image of a face for a single facial recognition technology use. The aggregation of biometric identification data with other sources of data supports new AI innovations in criminal enforcement[52] and national security contexts, such as biometric cyberintelligence and biometric-enabled warfare.[53] The type of AI-enabled evidence that can be derived from biometric AI include correlative evidence and predictive findings, for example, facial recognition technology that purports to serve as a form of identity verification as well as predictive of criminal or terrorist intent. Additionally, database screening can also deploy algorithms that are a part of a biometric AI architecture.[54] Cyber searches and data seizures can result in Fourth Amendment harms through the surveillance and AI analytics. Analysis of biometrics data fed into other AI-driven risk assessment can lead to AI-driven surveillance tools that erode or infringe upon reasonable

---

51. *See, e.g.*, Margaret Hu, *Orwell's* 1984 *and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1824 (2018).

52. *See, e.g.*, CLARE GARVIE ET AL., GEO. L. CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA 1 (2016), https://www.perpetuallineup.org; Ferguson, *Facial Recognition*, *supra* note 5; Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 CONN. L. REV. 1591, 1594 (2017); Brenda Leong, *Facial Recognition and the Future of Privacy: I Always Feel Like . . . Somebody's Watching Me*, 75 BULLETIN ATOMIC SCIENTISTS 109, 109 (2019); Katelyn Ringrose, Comment, *Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns*, 105 VA. L. REV. ONLINE 57, 59–61 (2019).

53. *See generally, e.g.*, ANNIE JACOBSEN, FIRST PLATOON: A STORY OF MODERN WAR IN THE AGE OF IDENTITY DOMINANCE (2021); Margaret Hu, *Biometric Cyberintelligence and the Posse Comitatus Act*, 66 EMORY L.J. 697 (2017).

54. *See, e.g.*, Elazar Zadok, *Legislative and Ethical Questions Regarding DNA and Other Forensic "Biometric" Databases*, *in* ETHICS AND POLICY OF BIOMETRICS 37 (Ajay Kumar & David Zhang eds., 2010); *see also* citations *supra* notes 5, 10–12, 16–19, 53, 54.

expectation of privacy protections, such as those asserting privacy to facial recognition technologies and geolocation privacy under the Fourth Amendment.[55]

Under the Fifth Amendment, many experts have focused on AI and the risk of procedural due process deprivations.[56] However, increasingly biometric AI also raises self-incrimination concerns. Returning to the example of facial recognition technology, in one case, a magistrate judge denied an application for a search warrant that would have compelled unlocking digital devices through biometric identification such as facial recognition and digitally stored fingerprints.[57] The court denied the application on the grounds that compelling the production of biometric data would violate the Fifth Amendment privilege against self-incrimination.[58] The reasoning of the order denying the application analogized the forced compulsion of participation in biometric AI, such as the type of biometric AI used in the security features of digital devices, to forced production of passwords.[59]

Andrea Roth contends that machine testimony poses particular concerns under the Sixth Amendment and, in particular, challenges the protections of the Confrontation Clause.[60] The Confrontation Clause allows for a criminal defendant to confront witnesses and evidence used against them.[61] "[I]n criminal cases, machine sources of accusation—particularly proprietary software created for litigation—might be 'witnesses against' a defendant under the Confrontation Clause."[62] AI-driven determinations introduced as evidence

---

55. *See generally, e.g.*, Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016).

56. *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1253 (2008); Margot E. Kaminski & Jennifer M. Urban, *The Right to Contest AI,* 121 COLUM. L. REV. 1957, 1989 (2021).

57. Matter of Residence in Oakland, California, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019).

58. *Id.* at 1016.

59. *Id.* at 1015. Several publications have discussed the potential impact of the case *Matter of Residence in Oakland, California*, and the issues of forcing compulsion of biometrics to bypass biometric authentication. *See, e.g.*, Ariel N. Redfern, Comment, *Face It—The Convenience of A Biometric Password May Mean Forfeiting Your Fifth Amendment Rights*, 125 PENN ST. L. REV. 597, 626 (2021); Adam Herrera, Comment, *Biometric Passwords and the Fifth Amendment: How Technology Has Outgrown the Right to Be Free from Self-Incrimination*, 66 UCLA L. REV. 778 (2019); *see also* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 778–82 (2019); *contra* Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 TEX. L. REV. ONLINE 73, 73–75 (2019).

60. Roth, *supra* note 5.

61. U.S. CONST. amend. VI.

62. Roth, *supra* note 5, at 1983 (citing *contra* Brian Sites, *Rise of the Machines: Machine-Generated Data and the Confrontation Clause*, 16 COLUM. SCI. & TECH. L. REV. 36, 99–100 (2014)).

in criminal law processes raise so-called "black box" concerns.[63] For example, the inscrutability of predictive analytics and correlative determinations through big data assessments has led to concerns of whether AI harms in a criminal proceeding can be adequately protected by the Sixth Amendment with an appropriate "confrontation" when the AI itself has little explanatory power.[64]

AI tools that use biometrics to identify individuals are known to be fallible, and are not guaranteed methods of identification.[65] Inaccurate facial recognition matches have led to wrongful arrests and jail time, while poor handling of DNA evidence have led to the same.[66] For instance, Amazon's facial recognition tool "Rekognition," when used on members of the U.S. Congress, falsely matched twenty-eight sitting legislators with mugshots.[67] The same issues of innate fallibility combine with issues of overconfidence in AI tools and inadequate understanding of the results by juries, judges, and even prosecutors.[68]

Further, facial recognition tools have been shown to lead to racially biased results, with people of color being disproportionately matched incorrectly more frequently than others.[69] This is just one example of algorithmic bias present in AI tools trained from a

63. Roth, *supra* note 5, at 1978.

64. *Id.* at 2048–50.

65. *See* Bess Stiffelman, *No Longer the Gold Standard: Probabilistic Genotyping Is Changing the Nature of DNA Evidence in Criminal Trials*, 24 BERKELEY J. CRIM. L. 110, 131 (2019); Drew Harwell, *Amazon Facial-Identification Software Used by Police Falls Short on Tests for Accuracy and Bias, New Research Finds*, WASH. POST (Jan. 25, 2019), http://www.washingtonpost.com/technology/2019/01/25/amazon-facial-identification-software-used-by-police-falls-short-tests-accuracy-bias-new-research-finds/.

66. Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES (Jan. 26, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html; Katie Worth, *Framed for Murder By His Own DNA*, THE MARSHALL PROJECT (Apr. 19, 2018, 7:00 AM), https://www.themarshallproject.org/2018/04/19/framed-for-murder-by-his-own-dna.

67. Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU (2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

68. *See, e.g.*, Victor Nicholas A. Metallo, *The Impact of Artificial Intelligence on Forensic Accounting and Testimony—Congress Should Amend "The Daubert Rule" to Include a New Standard*, 69 EMORY L.J. ONLINE 2039 (2020). Important research has considered how technology such as innovations in forensic evidence can influence criminal justice procedures and impact outcomes. *See, e.g.*, Brandon L. Garrett & Peter J. Neufeld, *Invalid Forensic Science Testimony and Wrongful Convictions*, 95 VA. L. REV. 1, 5 (2009); Tamara F. Lawson, *Before the Verdict and Beyond the Verdict: The CSI Infection Within Modern Criminal Jury Trials*, 41 LOY. U. CHI. L.J. 119 (2009); Andrea Roth, *Safety in Numbers? When DNA Alone is Enough to Convict*, 85 NYU L. REV. 1130 (2010); Laurie Meyers, *The Problem with DNA*, APA MONITOR, June 2007, at 52.

69. Snow, *supra* note 67.

homogenous sample set.[70] More extensive audits found that there were facial recognition tools that "reduced accuracy disparities" relating to race and gender, but such disparities were still present.[71]

Another way that racial disparities in biometric analysis by AI tools leads to actual disparities in justice outcomes is through the application of predictive policing systems.[72] Predictive policing aims to distribute police resources more efficiently to areas at times where crime is more likely to happen based on patterns discerned by AI through historical records. But, like other fallible AI tools, datasets used to generate predictive policing AI suffer from historical biases that leads to greater policing in neighborhoods with greater minority populations.[73] Predictive policing systems now target specific individuals that have been ascertained to be "at risk" of causing violent crimes.[74] The greater the power of these predictive policing systems become, the greater the drive will be to collect more data to further their application and power, including the collection of biometric data to integrate facial recognition and DNA in surveillance and prediction systems without proper transparency and security.[75]

It is also critical to observe the inherent limitations and challenges of AI tools when deployed as criminal evidence. AI evidence, once introduced, involves an explanation obstacle: the inability of the prosecution or its witnesses to explain how results are acquired by AI tools. This creates difficulties in interrogating the results of the tools to decide innocence or guilt. Source code of biometric analysis tools like DNA forensic software has been withheld by forensic software companies under IP protections of trade secret status.[76] Other times, the biometric analysis tools are based on an underlying AI that is a black box, typical of neural network machine-learning, whose decision making cannot be interrogated.[77] As a result,

---

70. *See, e.g.*, Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

71. *See, e.g.*, Inioluwa Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products in* PROCEEDINGS OF THE 2019 AAAI/ACM CONFERENCE ON AI, ETHICS, AND SOCIETY 429 (2019).

72. *See generally* Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109 (2017).

73. *See, e.g.*, Richardson et al., *supra* note 49.

74. *See, e.g.*, Ferguson, *Policing Predictive Policing*, *supra* note 72, at 1137–42.

75. *Id.* at 1167–68, 1186–87.

76. *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1358–62 (2018).

77. *See, e.g.*, Katherine Kwong, *The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence*, 31 HARV. J.L. & TECH. 275 (2017); Roth,

issues in discovery can arise where the AI "witness" cannot be readily "deposed" to explain the veracity of the results and outcomes.[78]

III. AI BILL OF RIGHTS

A. *Bill of Rights and Anticipating Biometric AI Harms*

The United States Bill of Rights was modeled on the English Bill of Rights of 1689,[79] the Declaration of Independence,[80] and various state constitutions to safeguard fundamental liberties,[81] limit government power, and to sustain a democratic form of governance.[82] Some of the rights enshrined in the Bill of the Rights were intended to be the rights of the people, or "collective and popular" rights.[83] Other rights were intended to be restraints on governmental power, for example, the first two amendments of the Bill of Rights safeguarded "the rights of popular majorities . . . against a possible unrepresentative and self-interested Congress."[84] The Bill of Rights served "as [a] beacon-light[] to guide and control the action of [state] legislatures, as well as that of Congress."[85]

Under any project undertaken to envision an AI Bill of Rights, it is appropriate to consider the protection of fundamental rights from biometric cybersurveillance harms. Recent empirical findings assessing United States public perspectives on biometric data collection and use across various contexts indicates that the United States citizenry is increasingly aware of potential privacy harms that can attach to biometric systems.[86] Just as the Bill of Rights was intended to constrain Congress and the states from unlawful

---

Safety in Numbers?, *supra* note 68; Jim Shook et al., *Transparency and Fairness in Machine Learning Applications*, 4 TEX. A&M J. PROP. L. 443, 448–449 (2018); Matthew Shaer, *The False Promise of DNA Testing*, ATLANTIC (June 2016), https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747/.

78. *See* Roth, *supra* note 5, at 2044–48.

79. *See, e.g.*, AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION, 25 n.25 at 24, 31–32, 60 (1998).

80. *See, e.g.*, *id.* at 106–09.

81. *See, e.g.*, *id.* at 30 ("In the Continental Congress's 1774 Declaration of Rights and in all six of the Revolutionary-era state constitutions affirming a right of the people to assemble, the right was explicitly yoked to the right of petition.") (citation omitted).

82. *See, e.g.*, *id.* at xii; *see also* CHRISTOPHER L EISGRUBER, CONSTITUTIONAL SELF-GOVERNMENT 2–3 (2001).

83. AMAR, *supra* note 79, at 30.

84. *Id.* at 21.

85. *Id.* at 154 (quoting Nunn v. Georgia, 1 Ga. 243, 251 (1846)).

86. Sara H. Katsanis et al., *U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics*, 3 IEEE TRANSACTIONS ON TECH. & SOC'Y 9 (2022), https://doi.org/10.1109/TTS.2021.3120317; Sara H. Katsanis et al., *A Survey of U.S. Public Perspectives on Facial Recognition Technology and Facial Imaging Data Practices in Health and Research Contexts*, PLOS ONE (2021), https://doi.org/10.1371/journal.pone.0257923.

infringements and encroachments, an AI Bill of Rights must function similarly to preserve individual rights and government restraint.

Biometric AI that is often deployed in criminal and terrorist screening is structured to serve both identification and risk assessment purposes.[87] Predictive analytics operationalize biometric-enabled AI systems that are structured to preempt crime and terrorism before they occur. Because these AI systems aim to identify data-driven suspects or suspicious data from an ocean of data, law enforcement and the intelligence community perceive biometric data as an anchor point, critically important for identity verification. Consequently, biometric cybersurveillance in the context of predictive policing and national security is critical to the project of envisioning how biometric AI stresses criminal procedure rights and other constitutional protections.[88]

B. Looking Ahead

As discussed above, the AI Act proposed by the EU explicitly links AI technologies, biometric identification, and the risk to fundamental rights.[89] Some question whether the AI Act will accomplish the regulatory goals set forth by the draft to provide a sufficiently robust framework to prevent AI harms to fundamental rights.[90] Whether the AI Act may or may not be crafted in a way that can achieve its goals, the proposed law's recognition of the extent of potential harms that biometric AI systems may inflict is instructive in envisioning the need for an AI Bill of Rights.

Similarly, the EU's General Data Protection Regulation ("GDPR") could also be useful in informing how best to shape new Bill of Rights protections.[91] First, the GDPR considers the need to

---

87. Hu, *Crimmigration-Counterterrorism*, *supra* note 19, at 991–93.

88. *See, e.g.*, Hu, *Algorithmic Jim Crow*, *supra* note 19; Hu, *Crimmigration-Counterterrorism*, *supra* note 19; Michael Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PENN. L. REV. 871 (2016); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Sohayla M. Roudsari, *Fourth Amendment Jurisprudence in the Age of Big Data: A Fresh Look at the "Penumbras" Through the Lens of Justice Sotomayor's Concurrence in United States v. Jones*, 9 FED. CTS. L. REV. 139, 140 (2016).

89. Khari Johnson, *The Fight to Define When AI is 'High Risk'*, WIRED (Sept. 1, 2021, 8:00 AM), https://www.wired.com/story/fight-to-define-when-ai-is-high-risk/; *see* discussion *supra* Part II.A.

90. *See, e.g.*, Natasha Lomas, *Europe's AI Act Falls Far Short on Protecting Fundamental Rights, Civil Society Groups Warn*, TECHCRUNCH (Nov. 30, 2021, 10:55 AM), https://techcrunch.com/2021/11/30/eu-ai-act-civil-society-recommendations/.

91. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data

frame data rights as a form of individual rights. For instance, GDPR's Articles 13–15 focus on a data subject's right to access data,[92] and Articles 21 and 22 address a data subject's right to object to and opt out of automated decision-making.[93] Next, facial recognition technology falls within the GDPR's regulation of both personal data and biometric data. Personal data is defined as: "any information relating to an identified or identifiable natural person ('data subject')" and encompasses both direct and indirect forms of identification."[94] Biometric data is defined as: "personal data resulting from specific technical processing relating to the physical . . . characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images . . . ."[95] Finally, the processing of personal data under the GDPR requires that it be undertaken in a "lawful, fairly, and . . . transparent manner[.]"[96] The GDPR, as a precursor to the proposed AI Act, demonstrates one model of how to restrain biometric AI system harms by embedding data rights within an AI Bill of Rights.

The EU's model of AI regulation, emphasizing transparency and greater accountability, is instructive in framing how best to protect criminal procedure protections afforded under the Sixth Amendment. The Sixth Amendment mandates that a defendant be "informed of the nature and cause of the accusation" and the Confrontation Clause guarantees a right to know one's accusers.[97] Under an AI Bill of Rights, those accused could be guaranteed the right to know the source of the data collected and used, the nature of the algorithm, and the interpreter of the AI-enabled outcome—to be "informed of the nature and cause of the accusation."[98] Guaranteeing the right to confront the AI forms the foundation of the tools of defense of the accused in cases where the prosecution relies upon AI evidence.

In short, the project of imagining an AI Bill of Rights benefits from a comparative approach to biometric data and biometric AI system regulation in the EU. The GDPR greatly expands the potential for better regulating biometric AI systems, already categorized as "high-risk" systems and "unacceptable risk" systems by the

---

and on the Free Movement of Such Data, 2016 O.J. (L119), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

92. *Id.* at arts. 13–15.
93. *Id.* at arts. 21, 22.
94. *Id.* at art. 4(1).
95. *Id.* at art. 4(14).
96. *Id.* at art. 5(1)(a).
97. U.S. CONST. amend. VI.
98. *Id.*

EU's proposed AI Act.[99] In recognizing the strain biometric AI systems are placing on criminal procedure protections under the Fourth, Fifth, and Sixth Amendments—as well as better understanding that biometric AI systems require additional oversight due to an expanding impact on fundamental rights—it is critical to look to the EU for greater guidance in how to construct AI Bill of Rights protections.

Already in the United States, reform efforts are underway that recognize the need for greater regulation of AI and high-risk biometric systems such as facial recognition systems used in law enforcement contexts.[100] During the 116th Congress, several bills were introduced to address federal uses of facial recognition technology. For example, a Senate bill proposed to create a moratorium on facial recognition technology pending a Commission study to assess its impact,[101] and also to impose warrant requirements upon federal law enforcement for searches utilizing facial recognition technology.[102] However, to date, federal legislation does not provide additional oversight for facial recognition technology uses by law enforcement.[103] States and local jurisdictions are increasingly considering bans on facial recognition technology. Portland, Maine, for example, banned city government officials from "using or authorizing the use of any facial surveillance software on any groups or members of the public . . . ."[104] States such as Illinois, Texas, and Washington have passed laws restricting biometric use and protecting biometric privacy.[105] Other states are proposing efforts to

---

99. EU 2021 Artificial Intelligence Act Proposal, *supra* note 7.

100. *See, e.g.*, JAMES A. LEWIS & WILLIAM CRUMPLER, CTR. STRATEGIC & INT'L STUDS., FACIAL RECOGNITION TECHNOLOGY: RESPONSIBLE USE PRINCIPLES AND THE LEGISLATIVE LANDSCAPE 5–6 (2021), https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape.

101. Ethical Use of Facial Recognition Act, S. 3284, 116th Cong. (2020) (introduced by Sen. Jeff Merkley (D-Ore.) and Sen. Cory Booker (D-NJ)) (not passed).

102. LEWIS & CRUMPLER, *supra* note 100 (citing Facial, Analysis, Comparison, and Evaluation Protection Act, H.R. 4021, 116th Cong. (2019) (introduced by Rep. Eliot Engel (D-NY-16), Rep. Eleanor Holmes Norton (D-DC), Rep. Nydia Velázquez (D-NY-7), Rep. Debra A. Haaland (D-NM-1), and Rep. José Serrano (D-NY-16) (not passed))).

103. *Id.* app. at 17.

104. Brian Heater, *Portland, Maine Passes Referendum Banning Facial Surveillance,* TECHCRUNCH (Nov. 4, 2020, 12:05 PM), https://techcrunch.com/2020/11/04/portland-maine-passes-referendum-banning-facial-surveillance/.

105. *See* Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/1–99; TEX. BUS. & COM. CODE ANN. § 503.001 (regulating "Capture or Use of Biometric Identifier"); WASH. REV. CODE §§ 19.375.010–.900 (regulating "Enrollment, Disclosure, and Retention of Biometric Identifiers"); *see also, e.g.*, LEWIS & CRUMPLER, *supra* note 100; *The Evolution of Biometric Data Privacy Laws*, BLOOMBERG L. (Nov. 4, 2021), https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws-and-lawsuits/. Other state laws such as the California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–.199.95, and the California Privacy Rights Act, A.B. 1490, 2021–2022 Leg., Reg. Sess. (Cal. 2021), are not solely biometric privacy laws, however,

specifically study facial recognition and AI technologies, and its impact. The Virginia General Assembly, for instance, proposed House Joint Resolution No. 59, calling for the formation of a Joint Commission on Technology and Science to study and report on "the proliferation and implementation of facial recognition and artificial technology within the Commonwealth."[106] The resolution reasoned that "facial recognition implicates constitutional concerns related to unreasonable searches and seizures [under the Fourth Amendment] as well as individual privacy[.]"[107] To date, the resolution has not passed.[108] The lack of a unified legislative approach at the federal level, combined with the increasing disunity of state and local approaches, to the regulation of biometric data and biometric AI systems, underscores the need for an AI Bill of Rights, a framework of rights that is capable of complementing and buttressing statutory developments or administrative oversight through other laws and regulations.

CONCLUSION

Biometric AI systems are increasingly being developed for a wide range of governmental purposes, including policing, border security and immigration enforcement, and biometric cyberintelligence and biometric-enabled warfare. Collection of biometric data in the criminal procedure context can exacerbate preexisting harms, such as historic over-policing of minority communities. AI analysis of biometric data has been known to be flawed in several cases, potentially aiding law enforcement, investigators, and prosecutors in their work, but also introducing sources of bias, and commonly understood AI fallibilities.

Better understanding the impact of biometric AI systems will be critical to the project of developing an AI Bill of Rights.[109] As signaled by the EU Commission's proposed AI Act, public and private uses of biometric identification systems carry increasing risks: the more comprehensive and ambitious biometric AI technologies are

---

also encompass biometric data protections. *The Evolution of Biometric Data Privacy Laws*, *supra* note 105.

106. H.J.R. 59, 2020 Gen. Assemb., Reg. Sess. (Va. 2020) (introduced by Del. Lashrecse D. Aird (D-Petersburg)).

107. *Id.*

108. *Legislation Related to Artificial Intelligence*, NAT'L CONF. STATE LEGISLATURES (Jan. 5, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx.

109. *See* Eric Lander & Alondra Nelson, *Americans Need a Bill of Rights for an AI-Powered World*, WIRED (Oct. 8, 2021), https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/.

in scope, the greater the risks are to the protection of fundamental rights. Both the proposed AI Act and the GDPR combined offer important ways to construct the types of rights and values necessary for an effective AI Bill of Rights, including the need to conceptualize data rights as fundamental rights and how biometric AI systems can infringe upon criminal procedure rights.

By closely examining the sweeping biometric collection proposed in the September 2020 NPRM in the final weeks of the Trump administration,[110] this Article suggests that the rapid expansion of biometric collection by DHS is also a case study for the expansive ambition of AI by the government generally. Without explicit acknowledgment of biometric AI system risks, the potential harms of attempts to broaden biometric data definitions and increase the collection of biometric data, and the potential ability to embed biometric data into emerging AI systems for multiple domestic and national security programs may be misunderstood. DHS is not only one of the primary drivers of expansion of biometric data collection, but also a driver of AI-enabled biometric cybersurveillance: biometric AI systems that rely upon biometric identifiers to anchor predictive policing and risk assessment profiling under purported border security and national security justifications. Beyond identity verification purposes, biometric AI systems are deployed to aggregate and analyze individuals and groups to conduct social scoring and project risk, to serve evidentiary and prosecutorial purposes, and to inform actionable intelligence.

AI-enabled biometric cybersurveillance carries the risk of substituting new technologies in place of traditional criminal evidence that criminal procedure protections under the Bill of Rights might not be able to sufficiently address. This Article concludes that a failure to recognize these challenges will lead to an underappreciation of the constitutional threats posed by emerging biometric AI systems. The growing recognition that high-risk biometric AI systems can pose unprecedented challenges to criminal procedure rights is core to the project of conceptualizing the need for an AI Bill of Rights.

110. Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, 85 Fed. Reg. 56338 (proposed Sept. 11, 2020).