Biometrics and AI Bias

I. Background: Physical Characteristics as Biometrics

WHILE humans share many physical characteristics, they are not replicas of one another in appearance. Despite their uniqueness, common features mean that comparisons can be made. The ability to identify someone by face has been one of the most fundamental ways that humans have connected with each other as distinct persons [1]. Recognizing someone is in fact a form of human visual information processing [2]. Long before mirrors were available in the ancient world (circa 5th century BCE the Greeks used hand mirrors for grooming [3]), descriptions of one's face were always determined by another's gaze or at best one's own description of their reflection in clean water illuminated by sunlight. Some even gained nicknames through the identification of distinct features on their forehead, nose, eyes, eyebrows, ears, and cheeks, for example, or through some clear markings, such as freckles or a birthmark. These were all the usual ways of remembering individuals; not as a means of discrimination but simply for the purposes of identification. In villages that did not exceed 250 households, it was possible to know of, and remember everyone [4], especially given that relations possessed similar and familial features.

Today, we refer to these distinct physical characteristics as biometrics [5]. We have used biometrics such as fingerprints to denote uniqueness since the turn of the 1900s (e.g., Scotland Yard introduced the Galton–Henry system of fingerprint classification published in June 1900 [6]). By the mid-1980s, U.S. law enforcement had automated fingerprint matching, and by the 1990s, 500 automatic fingerprint identification systems (AFIS) were used to convict people of crimes [7]. The implementation of AFIS marked the first time that automation had been used to cross-check minutiae. Presently, millions of minutiae have been gathered worldwide using high-resolution cameras, away from traditional ink-based methods (e.g., in India, the world's largest biometric ID system, known as Aadhaar, has systematically collected over a billion fingerprints). Interpol's AFIS alone has 220 000 fingerprint records from more than 17 000 crime scene marks, conducting 3000 comparisons a day [8]. Commensurately, it has only been in the last two decades that automated facial recognition has become possible and prevalent for a variety of applications, such as unlocking phones, locating missing persons, reducing retail crime, and even tracking student and worker attendance among other applications [9].

Digital Object Identifier 10.1109/TTS.2022.3156405

II. Automated Facial Recognition Systems

Some of the earliest automated biometric recognition systems of the 1980s could be described at best as clunky. They required specialist stand-alone hardware with limited computational power, and algorithms that matched on a small number of given attributes with a limited record sample in their databases, compared to today's large number of attributes which contain, in some cases, billions of images [10, ch. 6.5]. Consider the face, as an intricate map of which distinguishing features are registered and compared with other records in a database [11]. Biometrics measure distinctiveness, seeking variations in biometric patterns among the general population. The higher the distinctiveness of a feature, the more unique the identifier to the individual [12]. Thus, facial biometrics relies on spatial geometry to denote measures of key features of the face.

Automated facial recognition systems are broadly comprised of four stages: 1) face detection (e.g., through the use of CCTV footage); 2) face analysis (2-D and 3-D captures are possible, although most captured images are typically 2-D, with 3-D predicted to have a significant impact in the future); 3) image to data conversion (using a very complex mathematical formulae); and 4) comparison and matching [13]. It is in the second stage where measurements are taken of the distance between the eyes, from the forehead to the chin, the cheekbones, contours of the lips, ears, and chin, in addition to the depth of eye sockets [14]. The aim of this analysis is akin to finding distinct points of interest on a map, where each facial image is converted into a faceprint (a unique profile of 1s and 0s). When a faceprint is compared against a large database of other faceprints, statistics are used to glean which "near matches" might be worth considering for further investigation and scrutiny [15].

Statistics have always played a key role in identifying approximate biometric matches, where a given match on a "hit" (i.e., a suspect) was required in resolving a criminal investigation [16]. Low-resolution surveillance footage was at times the only available evidence for the police near a crime scene, especially when the suspect was not previously known to authorities. Very low-light levels, off-angle, atmospheric conditions (e.g., rain or fog), and other camera noise [17] also add to the complexity of using photographic evidence to make a conviction or even an arrest. Digital facial images are rarely used on their own, without direct eyewitness evidence. However, in the absence of eyewitness accounts, CCTV footage may well be the only available data to bring a criminal to justice, especially in the context of a heinous crime where the use of automated biometric recognition is deemed proportional to the crime committed. Today, firmware updates have added capabilities to even the lowest resolution surveillance

2637-6415 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

camera systems making them more "intelligent" [18], through advancements in deep learning algorithms based on neural nets, in addition to increasing levels of interconnectedness over the cloud allowing for image sharing at scale [19].

Biometrics vendors increasingly tout an impossible "near 99%" exact facial image case match, claiming to utilize the additional capability of Web scraping (of images) from the Internet, social media platforms, and more to enhance their results [20]. But does more data necessarily mean better outcomes? It all depends on the quality of the data gathered and of the data matched against. The possibility of entangling innocent people in suspect lists and even wrongful arrests [21] is higher than ever before, as a result of the connected nature of social networks and Internet-based traffic. If I exist and have presented in a public space (physical or online), then the chance that my face will be stored on the cloud is not only high but inevitable, whether or not I have granted consent for that image to be collected and retained [22]. However, there are also reported benefits; that is, this very ability to match against public images has provided a fresh avenue to solve crimes in a manner that accounts for individuals who are not on criminal databases, and would never have otherwise come to the attention of authorities via a match [23].

III. Citizen Rights, Public Spaces, and Informed Consent

But what is the cost of increased biometric data collection in public spaces? Here, we are not referring to the cost of upgrading an aging surveillance camera or other operational costs, but rather the human cost with respect to innocent people presenting on suspect lists via dragnet-style facial recognition searches [24]. To date, a number of U.S. cities [25], including Boston, Portland, and San Francisco have moved to ban facial recognition systems in their neighborhoods as a means of addressing human costs. From an organizational perspective, the State of Illinois has banned the corporate use of biometrics systems through the biometric information privacy act (BIPA) [26]. The matter of appropriate regulation surrounding these biometric systems has now become part of major legal and policy debates throughout the world [27]. For example, see the recent bill introduced by U.S. Senators Wyden, Booker, and Clarke, known as the "Algorithmic Accountability Act of 2022". How to maintain one's privacy despite the automated process of data gathering and collection of facial images, is a question that must be addressed [28], [29], [67]. "Who owns information?" as Ann Branscomb asked in 1994 [30], has taken on new meaning since the advent of Web 2.0, 5G mobile, advances in storage area networks and new ways to analyze the data collected through emergent approaches in artificial intelligence and machine learning (ML) [68]. Soft biometrics, which provides an additional layer of description, can also infer a great deal about someone using qualitative attributes, by capturing data about the way an individual might style their hair or wear a beard; use hats, scarfs, or eye glasses; and even capture data about their attire including the type, brand, and color of clothes; the make-up applied; other apparel adorned such as earrings and necklaces, and much more [31].

As greater urbanization occurs toward the formation of megacities, smart cities development through digital transformation will also continue to evolve, as will the ability to collect additional data relevant to individuals through Internet of Things (IoT)-based systems and other related infrastructure. The ability to uniquely identify a person, by their face or gait, and even determine their probable emotional state simply via their facial expressions [32], will almost certainly give rise to a myriad of new emerging capabilities without the use of a token, and most likely without informed consent. Facial and musculoskeletal images have been scrutinized for decades in the early diagnosis of medical conditions, such as Turner Syndrome [33] and Noonan Syndrome, in addition to more recent attempts at detecting schizophrenia [34] or even for diagnosing whether someone is on the autism spectrum [35]. The extension of this, facilitated by the identified technological developments, is evident in a range of contexts. For instance, employers can now analyze worker moods and even remote productivity through a variety of biometric data they gather via specialist software on company laptops and other proximate devices [36], [37].

IV. Machine Learning and AI Bias

Digitalization and datafication processes are not new. The world has been gradually undergoing digital transformation, especially since the introduction of transaction processing, enabling data to be entered and stored as records in databases that could be used for report generation and inquiry processing activities. Today, as big datasets have been amassed by corporations, government and law enforcement agencies, ML is increasingly being utilized. ML is the process by which software can automatically detect matches, meaningful patterns and trends in large troves of data (e.g., facial images). It also allows for the automatic detection and verification of a face in a biometric image search. But identifying people by the way they look is not as simple as it might sound [38]. People change over time, either through the natural aging process or by changes in fashion (including hair cuts, facial hair, make-up, clothing, and accessories) or other aesthetic changes like plastic surgery [39], [40].

Increasingly, high-quality images such as those found in driver's license state databases and passport photographs have been utilized by government agencies for identity matching, for example, in bushfire situations in Australia [41]. But there is still a considerable proportion of the population that do not drive and have never traveled overseas. This results in numerous questions that require exploration, such as what happens to people who have neither credential? And how will a person be treated if found to be an exception? There are also questions surrounding how many matches may be returned in given search algorithms in the context of verification versus identification (i.e., an alleged one-to-one match as opposed to a one-to-many match of an unknown person with an established identity in a government database). Similar challenges arise in other applications of AI in diverse contexts. In the workplace, for instance, facial recognition is becoming more evident, especially in candidate matching and recruitment. AI-backed platforms such as Paññã (https://www.panna.ai/)

enable companies to process video content such as online interviews to determine whether a candidate is potentially cheating by reading a script or listening to cues from someone off-screen. These algorithms look for aberrant behaviors based on eye movement, facial expressions, and more. However, prevalent questions arise in this scenario, such as: is there adequate diversity in the original training dataset to capture and interpret facial expressions of people from diverse cultural backgrounds? Can the algorithm capture the complexity in the environment, for example, in cases where the interview is held in a noisy or public space? Hence, any potential biases or limitations in the algorithms can result in the misinterpretation of behaviors, potentially leading to discrimination.

Recognizing the many limitations of ML and the hidden assumptions pertaining to "the dark side" of AI [66], as well as traditional challenges related to biometrics, is critical. For example, false acceptance rates (FARs) and false rejection rates (FRRs) are still common in biometric systems [42]. This begs a series of additional questions: should we be automating critical service provisioning utilizing technology in this way (e.g., for emergency patient identification)? What is the role of ethics in these situations, specifically in relation to privacy, autonomy, informed consent, and responsibility? Is it possible to think of a future smart city, where an elderly person who might be wandering in the early stages of dementia, can be reunited with family or their caregivers if found roaming through multimodal gait and facial analysis? And what are the implications in view of algorithmic bias?

In the context of this special issue, the bringing together of facial image datasets and AI-based algorithms has been determined to lead to a variety of algorithmic biases "in context," including racial bias [43] and gender bias [44], although not all biases are demographic in nature [45]. Algorithmic bias occurs when "AI produces systematically unfair outcomes that can arbitrarily put a particular individual or group at an advantage or disadvantage over another" [42, p. 2]. Facial recognition systems in particular struggle with skin tone [46], gender identification, and many other attributes. Certain communities are discriminated against either because too much training data exists on that community historically, or not enough. This is an endemic issue in the original training dataset that has been collected, without adequate testing for sample representation [47], or even specified data annotation. Yet again, key questions are often left unanswered, such as what is the source of the data being used? When was it created? Who generated it? For what purpose? What does it mean? Akter *et al.* [48] went beyond mere "data," to describe three primary dimensions of bias that might pervade ML inclusive of design bias, contextual bias, and application bias, identifying subdimensions that are highly applicable to biometrics, such as model, method, cultural, social, and personal biases. Some of the most controversial research to be conducted to date perhaps [66], as pointed out by Bowyer *et al.* [49] is proving "criminality" by facial image [50]. This may well be considered the most extreme form of bias, to imagine that one's face can denote their criminality, or whether they would make a good rental tenant.

In order to ameliorate the risk of AI bias in biometric systems, algorithmic audits can be conducted to ensure algorithmic justice [51], [65] through comprehensive testing and validation, dependent on the choice of the algorithm used, which is very much linked to the application context. This will ensure that inclusivity and equity are addressed in discussions and decision-making processes. Racial bias, and gender bias, are prevalent in many commercial and government biometric systems and a number of nongovernment organizations (NGOs) are attempting to raise awareness of these problems. For example, the Algorithmic Justice League https://www.ajl.org/ that seeks to "build a movement towards equitable and accountable AI" [52]. Two seminal works that sparked numerous movements and raised awareness about biases in ML and their corresponding social implications included Cathy O'Neil's (2016) *Weapons of Math Destruction* [53] and Safiya Noble's (2018) *Algorithms of Oppression* [54]. Overcoming such AI-biases in biometrics requires diversity in the workplace; greater depth of testing and validation in the AI design, AI dataset, and AI model; a thorough assessment as to whether the application context is appropriate for use; and an awareness of emergent research and developments pertaining to the design of AI-based systems.

V. Areas of Future Research

There are many promising research areas relating to the design of biometric systems and ML algorithms to alleviate AI-biases. One such area is relevant to gender bias, where emerging evidence indicates that the overrepresentation of males in the creation of AI systems during the design phase leads to biases creeping in. This, in turn, impacts usability and engagement with this technology in inequitable ways, leading to further perpetuating learning, working and living spaces that disadvantage women [63]. While there is recognition that algorithmic justice can only be achieved through inclusivity in design of AI systems through participatory design processes, research and practice are in nascent stages with regard to achieving this goal. At a time when AI is transforming the way we engage with the world of work and play, it is crucial that researchers engage with narratives from women as leaders, consumers, users, and designers of technology [69]. The issue of pipeline block is well examined in gender studies, with substantive studies focusing on strategies at institutional and individual levels that are transforming women from engaged players to empowered change agents. There is an opportunity here for AI researchers to draw on this preliminary research on women and leadership and pipeline block [60], [64] to examine the biases that impact women's participation as equal players in the design process. For example, gender research indicates that particular forms of capital are valued in traditionally male dominant spaces, which advantages the dominant cohort, leading them to repeat the cycle of creating enabling contexts that attract and retain those who embody male prototypical capital [58], [59], [61]. Capital is defined by Bourdieu as "all goods, material and symbolic, without distinction, that present themselves as rare and worthy of being sought after in a particular social formation" [55, p. 78]. There is a need for a critical theory perspective to examine the kinds of capital (e.g., cultural and social psychological) that are valued in the design process, who the key players are, what the rules of the game are and what kinds of capital needs to be mobilized to achieve legitimacy.

While there is acknowledgement of gender bias in ML in research and practice, the body of knowledge is still very much in its early stages, with no known research yet on capital that is valued or the factors that impact capital creation processes in technology design. Given that capital creation processes are impacted by factors at micro, meso, and macro levels, there is also a need for taking a holistic and multistakeholder lens to advance gender theory in AI. Specifically, there is a need for examining inclusivity in AI that acknowledges divergent stakeholder interests and takes an interdisciplinary and complete view of the ecosystem of AI design through focusing on endogenous and exogenous factors. In particular, research can draw on the factors impacting emergence and enactment of leadership among women in AI by drawing on related literature in women and leadership [56], [57], [62] to develop theory and practice that support the advancement of women's careers in AI. Furthermore, additional biases identified throughout this editorial require equal and detailed consideration, from the perspective of design.

VI. Overview of Accepted Papers

Four papers are featured in this special issue on "Biometrics and AI Bias." The first paper by Katsanis *et al.* brings together ten coauthors and is titled: "U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics." This is a timely piece that will contribute to existing scholarship empirical evidence required to inform policy debates, depending on the level of sensitivity of given communities. The authors were supported in this work in part by the National Institutes of Health (NIH) Office of the Director (OD) and in part by the National Institute of Dental and Craniofacial Research (NIDCR) under Grant 3R01DE027023-04S1. The work of Katsanis was also partially supported by the National Human Genome Research Institute (NHGRI) under Grant R01HG009923, and the work of Cook-Deegan was supported in part by the National Cancer Institute under Grant R01CA237118 and Grant U01CA242954. The project team of Katsanis, Claes, Doerr, Cook-Deegan, Tenenbaum, Evans, Keun Lee, Anderton, Weinberg, and Wagner is cross-disciplinary, with backgrounds in health, medicine, engineering, genetics, technology and innovation, biostatistics, law, and bioethics. They also have diverse employment in hospitals, academia, private enterprise and specialist centers.

The team explored the application of biometrics in the U.S. with an emphasis on facial recognition and DNA identification. Citing their substantial survey of over 4000 adults, they explored six types of biometrics; the level of comfort of applying biometrics to distinct scenarios; trust and responsible use of two types of biometrics; the level of acceptance of facial images in given scenarios; and finally, the perceived effectiveness of facial images for particular tasks. The study did not find sociodemographic factors to influence perspectives on biometrics in obvious ways, underscoring the need for qualitative approaches to understand the contextual factors that trigger strong opinions of comfort with, and acceptability of, biometrics in different settings, by different actors, and for different purposes. The team believes that these factors may well provide the information needed for the development of appropriate policies and oversight.

The second paper is titled, "A Comprehensive Study on Face Recognition Biases Beyond Demographics." The paper was written by Terhörst, Niklas Kolf, Huber, Kirchbuchner, Damer, Morales Moreno, Fierrez, and Kuijper. The eight authors were supported in part by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts with their joint support of the National Research Center for Applied Cybersecurity ATHENE, and in part by the Projects BIBECA under Grant RTI2018-101248-B-I00 MINECO/FEDER and PRIMA under Grant H2020-MSCA-ITN-2019-860315. The authors are from several organizations and institutions, the Department of Smart Living & Biometric Technologies, Fraunhofer Institute for Computer Graphics Research in Germany, and the Interactive Graphics Systems Group at the Technical University of Darmstadt. Morales Moreno and Fierrez are with the Biometrics and Data Pattern Analytics Lab at the Universidad Autonoma de Madrid in Spain.

Following on from the work of the first paper in this special issue, these authors now cast our attention to the use of face recognition systems and their growing effect on critical decision-making processes. The authors of this second paper maintain that while facial recognition solutions show strong performance differences, what is necessary is trustworthy facial recognition technology. In essence, this team embarked on analyzing the effect of 47 attributes implementing two popular facial recognition models (i.e., FaceNet and ArcFace), using the publicly available MAAD-Face1 annotation database that was based on VGGFace2, consisting of over 120M high-quality attribute annotations for 3.3M face images. The results of the study demonstrated that many nondemographic attributes strongly affected recognition performance, such as accessories, hairstyles and colors, face shapes, or facial anomalies. Plainly, the study showed that further research is required to make facial recognition systems more robust, explainable, and fair.

The third paper was an interdisciplinary effort by Dancy of the Computer Science Department and the Critical Black Studies Department at Bucknell University, alongside Saucier, the Chair of the latter department. Their paper titled: "AI and Blackness: Toward Moving Beyond Bias and Representation," hones in on "color" as an attribute as noted by the second paper in the special issue. Dancy and Saucier argue that AI ethics must move beyond the concepts of race-based representation and bias. The authors state that there must be further probing on the impact of facial recognition systems, and how they are designed, developed, and deployed. They state that while recent discussions have centered on racial bias caused by AI systems, we must go beyond the ethical considerations of bias and seek to focus on the examination of the ontological space that provides a foundation for the design of AI systems. This means that we need to consider the sociocultural contexts from the outset if we are to have any hope in creating systems that do not discriminate. The authors provide evidence for their argument by auditing an existing opensource semantic network called ConceptNet.

The fourth and final paper in this special issue is from Parra and Gupta from Florida International University, and Dennehy from Swansea University. This paper addresses the racial bias as in the case of the third paper written by Dancy and Saucier, and also introduces the concept of gender bias. While the first paper in the special issue used surveys, the second paper applied two models to 3.3M facial images, and the third paper audited the opensource semantic network called ConceptNet looking specifically at racial bias, this final paper used a scenario-based survey issued to 387 U.S. participants to explore when individuals in given daily life circumstances would be more likely to question the racial bias and gender bias in the context of AI-based online recommendations.

KATINA MICHAEL, *Editor-in-Chief*
School for the Future of Innovation in Society
Arizona State University
Tempe, AZ 85287 USA
E-mail: katina.michael@asu.edu

ROBA ABBAS, *Co-Editor*
School of Business
University of Wollongong
Wollongong, NSW 2522, Australia
E-mail: roba@uow.edu.au

PAYYAZHI JAYASHREE
Faculty of Business
University of Wollongong Dubai
Dubai, UAE
E-mail: payyazhijayashree@uowdubai.ac.ae

RUWAN J. BANDARA
Faculty of Business
University of Wollongong Dubai
Dubai, UAE
E-mail: ruwanbandara@uowdubai.ac.ae

ANAS ALOUDAT
Faculty of Business
University of Jordan
Amman, Jordan
E-mail: a.aloudat@ju.edu.jo

REFERENCES

[1] K. Sutherland, D. Renshaw, and P. B. Denyer, "Automatic face recognition," in *Proc. 1st Int. Conf. Intell. Syst. Eng.*, 1992, pp. 29–34.
[2] R. J. Baron, "Mechanisms of human facial recognition," *Int. J. Man-Mach. Stud.*, vol. 15, no. 2, pp. 137–178, 1981.
[3] M. M. Lee, *Body, Dress, and Identity in Ancient Greece*. New York, NY, USA: Cambridge Univ. Press, 2015.
[4] R. I. M. Dunbar, *How Many Friends Does One Person Need? Dunbar's Number and Other Evolutionary Quirks*. London, U.K.: Faber Faber, 2010.
[5] A. K. Jain, P. Flynn, and A. A. Ross, Eds., *Handbook of Biometrics*. New York, NY, USA: Springer, 2007.
[6] K. Michael and M. G. Michael, "Biometrics: In search of a foolproof solution," in *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*. Hershey, PA, USA: IGI Global, 2009, pp. 191–233.
[7] P. Komarinski, *Automated Fingerprint Identification Systems (AFIS)*. Amsterdam, The Netherlands: Elsevier, 2005.
[8] "Fingerprints." Interpol. [Online]. Available: https://www.interpol.int/en/How-we-work/Forensics/Fingerprints (accessed Feb. 27, 2022).
[9] J. D. Woodward, Jr., C. Horn, J. Gatune, and A. Thomas, *Biometrics: A Look at Facial Recognition*. Santa Monica, CA, USA: RAND Corp., 2003.
[10] K. Michael, "The technological trajectory of the automatic identification industry: The application of the systems of innovation (SI) framework for the characterisation and prediction of the auto-ID industry," Ph.D. dissertation, Dept. School Inf. Technol. Comput. Sci., Univ. Wollongong, Wollongong, NSW, Australia, 2003. [Online]. Available: http://ro.uow.edu.au/theses/309
[11] V. Bruce and A. Young, "Understanding face recognition," *Brit. J. Psychol.*, vol. *77*, no. 3, pp. 305–327, 1986.
[12] J. D. Woodward Jr., C. Horn, J. Gatune, and A. Thomas, *Biometrics: A Look At Facial Recognition*. Santa Monica, CA, USA: RAND Corp., 2003, pp. 3–4.
[13] "What Is Facial Recognition—Definition and Explanation." Kaspersky.com. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition (accessed Feb. 27, 2022).
[14] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Comput. Surv.*, vol. 35, no. 4, pp. 399–458, 2003.
[15] R. Jafri and H. R. Arabnia, "A survey of face recognition techniques," *J. Inf. Process. Syst.*, vol. 5, no. 2, pp. 41–68.
[16] J. W. Tanaka and M. J. Farah, "Parts and wholes in face recognition," *Quart. J. Exp. Psychol.*, vol. 46, no. 2, pp. 225–245, 1993.
[17] Z. Cao, X. Cen, H. Zhao, and L. Pang, "Balancing heterogeneous image quality for improved cross-spectral face recognition," *Sensors*, vol. 21, no. 7, p. 2322, 2021. [Online]. Available: https://doi.org/10.3390/s21072322
[18] K. Patel and M. Patel, "Smart surveillance system using deep learning and RaspberryPi," in *Proc. 8th Int. Conf. Smart Comput. Commun.*, Kochi, India, 2021, pp. 246–251, doi: 10.1109/ICSCC51209.2021.9528194.
[19] A. Vinay, V. S. Shekhar, J. Rituparna, T. Aggrawal, K. N. B. Murthy, and S. Natarajan, "Cloud based big data analytics framework for face recognition in social networks using machine learning," *Procedia Comput. Sci.*, vol. 50, pp. 623–630, Jan. 2015.
[20] K. O'Flaherty. "Clearview AI's Nightmare Just Got Worse: Here's Why It Matters." Forbes. Feb. 2020. [Online]. Available: https://www.forbes.com/sites/kateoflahertyuk/2020/02/28/the-clearview-ai-nightmare-just-got-worse-heres-why-it-matters-and-what-must-come-next/?sh=5412be422afd
[21] K. Hill. "Wrongfully Accused by an Algorithm." The New York Times. Jun. 2020. [Online]. Available: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html
[22] E. Mordini, "Nothing to hide biometrics, privacy and private sphere," in *Proc. 1st Eur. Workshop Biometrics Identity Manag.*, 2008, pp. 247–257.
[23] "Fed. Agency Identifies Suspect of Las Vegas Child Exploitation in Background of Social Media Profile." ClearView AI. [Online]. Available: https://www.clearview.ai/post/fed-agency-identifies-suspect-of-las-vegas-child-exploitation-in-background-of-social-media-profile (Accessed Oct. 15, 2021).
[24] D. A. Fretty, "Face-recognition surveillance: A moment of truth for fourth amendment rights in public places," *Virginia J. Law Technol.*, vol. 16, no. 3, p. 430, 2011.
[25] J. Lunter, "Beating the bias in facial recognition technology," *Biometric Technol. Today*, vol. 9, pp. 5–7, Oct. 2020.
[26] C. Pope, "Biometric data collection in an unprotected world: Exploring the need for federal legislation protecting biometric data," *J. Law Policy*, vol. 26, no. 2, p. 769, 2018.
[27] L. Introna and H. Nissenbaum, "Facial recognition technology: A survey of policy and implementation issues," Lancaster Univ. Manag. School, Lancaster, U.K., Working Paper 2010/030, 2009.
[28] M. Hirose, "Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology," *Connecticut Law Rev.*, vol. 49, no. 5, p. 1591, 2016.
[29] A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[30] A. W. Branscomb, *Who Owns Information? From Privacy to Public Access*. New York, NY, USA: Basic Books, Inc., 1994.
[31] A. Dantcheva, E. Petros, and R. Arun, "What else does your biometric data reveal? A survey on soft biometrics," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 441–467, 2015.
[32] E. Selinger and W. Hartzog. "What Happens When Employers Can Read Your Facial Expressions?" The New York Times. Oct. 2019. [Online]. Available: https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html
[33] Z. Pan *et al.*, "Clinical application of an automatic facial recognition system based on deep learning for diagnosis of Turner syndrome," *Endocrine*, vol. 72, no. 3, pp. 865–873, 2021.
[34] R. E. Gur *et al.*, "An fMRI study of facial emotion processing in patients with schizophrenia," *Amer. J. Psychiatry*, vol. 159, no. 12, pp. 1992–1999, 2002.
[35] M. B. Harms, A. Martin, and G. L. Wallace, "Facial emotion recognition in autism spectrum disorders: A review of behavioral and neuroimaging studies," *Neuropsychol. Rev.*, vol. 20, no. 3, pp. 290–322, 2010.
[36] E. A. Brown, "A healthy mistrust: Curbing biometric data misuse in the workplace," *Stanford Technol. Law Rev.*, vol. 23, pp. 252–298, Jun. 2020.
[37] I. Ajunwa, "Algorithms at work: Productivity monitoring applications and wearable technology as the new data-centric research agenda for employment and labor law," *St. Louis U. L.J.*, vol. 63, p. 21, Jul. 2019.
[38] A. Pentland, "Looking at people: Sensing for ubiquitous and wearable computing," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 1, pp. 107–119, Jan. 2000.
[39] B. Miller, "Vital signs of identity [biometrics]," *IEEE Spectr.*, vol. 31, no. 2, pp. 22–30, Feb. 1994.
[40] M. Nappi, S. Ricciardi, and M. Tistarelli, "Deceiving faces: When plastic surgery challenges face recognition," *Image Vis. Comput.*, vol. 54, pp. 71–82, Oct. 2016.
[41] L. Sleep and P. Harris, "The importance of digital inclusion in accessing care and support in our increasingly digitised world," *J. Soc. Inclusion*, vol. 12, no. 2, pp. 1–2, 2021.
[42] S. Akter, Y. K. Dwivedi, K. Biswas, K. Michael, R. J. Bandara, and S. Sajib, "Addressing algorithmic bias in AI-driven customer management," *J. Global Inf. Manag.*, vol. 29, no. 6, pp. 1–27, 2021.
[43] F. Bacchini and L. Lorusso, "Race, again: How face recognition technology reinforces racial discrimination," *J. Inf. Commun. Ethics Soc.*, vol. 17, no. 3, pp. 321–335, 2019. [Online]. Available: https://doi.org/10.1108/JICES-05-2018-0050
[44] A. Ross *et al.*, "Some research problems in biometrics: The future beckons," in *Proc. Int. Conf. Biometrics*, 2019, pp. 1–8.
[45] P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, "Demographic bias in biometrics: A survey on an emerging challenge," *IEEE Trans. Technol. Soc.*, vol. 1, no. 2, pp. 89–103, Jun. 2020.
[46] K. S. Krishnapriya, V. Albiero, K. Vangara, M. C. King, and K. W. Bowyer, "Issues related to face recognition accuracy varying based on race and skin tone," *IEEE Trans. Technol. Soc.*, vol. 1, no. 1, pp. 8–20, Mar. 2020.
[47] D. Castelvecchi, "Is facial recognition too biased to be let loose?" *Nature*, vol. 587, no. 7834, pp. 347–350, 2020.
[48] S. Akter, Y. K. Dwivedi, S. Sajib, K. Biswas, R. J. Bandara, and K. Michael, "Algorithmic bias in machine learning-based marketing models," *J. Bus. Res.*, vol. 144, pp. 201–216, May 2022.
[49] K. W. Bowyer, M. C. King, W. J. Scheirer, and K. Vangara, "The 'criminality from face' illusion," *IEEE Trans. Technol. Soc.*, vol. 1, no. 4, pp. 175–183, Dec. 2020. [Online]. Available: https://doi:10.1109/TTS.2020.3032321
[50] R. van Noorden, "The ethical questions that haunt facial-recognition research," *Nature*, vol. 587, no. 7834, pp. 354–359, 2020.
[51] A. Roussi, "Resisting the rise of facial recognition," *Nature*, vol. 587, no. 7834, pp. 350–354, 2020.
[52] S. Costanza-Chock, "Design justice, A.I., and escape from the matrix of domination," *J. Des. Sci.*, Jul. 2018. [Online]. Available: http://dx.doi.org/10.21428/96c8d426
[53] C. O'Neil, *Weapons of Math Destruction*. U.K.: Crown Publ. Group, 2016.
[54] S. Noble's, *Algorithms of Oppression*. New York, U.K.: New York Univ. Press, 2018.
[55] P. Bourdieu, *Outline of a Theory of Practice*. Cambridge, U.K.: Cambridge Univ. Press, 1977.
[56] A. H. Eagly, "Achieving relational authenticity in leadership: Does gender matter?" *Leadership Quart.*, vol. 16, no. 3, pp. 459–474, 2005.
[57] A. H. Eagly and S. J. Karau, "Role congruity theory of prejudice toward female leaders," *Psychol. Rev.*, vol. 109, pp. 573–598, Jul. 2002.
[58] T. W. Fitzsimmons and V. J. Callan, "Applying a capital perspective to explain continued gender inequality in the C-suite," *Leadership Quart.*, vol. 27, no. 3, pp. 354–370, 2016.
[59] J. Glover, D. Champion, K. Daniels, and G. Boocock, "Using capital theory to explore problem solving and innovation in small firms," *J. Small Bus. Enterprise Develop.*, vol. 23, no. 1, pp. 25–43, 2016.
[60] K. Hutchings, P. Lirio, and B. D. Metcalfe, "Gender, globalization and development: A re-evaluation of the nature of women's global work," *Int. J. Human Resour. Manag.*, vol. 23, no. 9, pp. 1763–1787, 2012.
[61] P. Jayashree, V. Lindsay, and G. McCarthy, "Career capital development of women in the Arab Middle East context: Addressing the pipeline block," *Pers. Rev.*, vol. 50, no. 4, pp. 1253–1278, 2020.
[62] A. M. Koenig, A. H. Eagly, and A. A. Mitchell, "Are leader stereotypes masculine? A meta-analysis of three research paradigms," *Psychol. Bull.*, vol. 137, no. 4, pp. 616–642, 2011.
[63] l. S. Leavy, "Gender bias in artificial intelligence: The need for diversity and gender theory in machine learning," in *Proc. ACM/IEEE 1st Int. Workshop Gender Equality Softw. Eng.*, Gothenburg, Sweden, 2018, pp. 14–16.
[64] Y. M. Sidani, A. Konrad, and C. M. Karam, "From female leadership advantage to female leadership deficit: A developing country perspective," *Career Develop. Int.*, vol. 20, no. 3, pp. 273–292, 2015.
[65] O. Marjanovic, D. Cecez-Kecmanovic, and R. Vidgen, "Theorising algorithmic justice," *Eur. J. Inf. Syst.*, to be published, doi: 10.1080/0960085X.2021.1934130
[66] P. Mikalef, K. Conboy, J. E. Lundström, and A. Popovič, "Thinking responsibly about responsible AI and 'the dark side' of AI," *Eur. J. Inf. Syst.*, to be published, doi: 10.1080/0960085X.2022.2026621.
[67] J. D. Woodward, "Biometrics: Privacy's foe or privacy's friend?" *Proc. IEEE*, vol. 85, no. 9, pp. 1480–1492, Sep. 1997.
[68] L. Chato and S. Latifi, "Application of machine learning to biometric systems—A survey," *J. Phys. Conf. Ser.*, vol. 1098, no. 1, 2018, Art. no. 12017.
[69] K. Michael, R. Abbas, and J. Pitt, "Maintaining control over AI," *Issues Sci. Technol.*, vol. 37, no. 3, 2021. [Online]. Available: https://issues.org/debating-human-control-over-artificial-intelligence-forum-shneiderman

Katina Michael (Senior Member, IEEE) received the B.S. degree in information technology from the School of Mathematical and Computing Science, University of Technology, Sydney, NSW, Australia, in 1996, the Doctor of Philosophy degree in information and communication technology from the Faculty of Informatics, University of Wollongong, NSW, Australia, in 2003, and the Master of Transnational Crime Prevention degree (Distinction) from the Faculty of Law, University of Wollongong in 2009.

She is with Arizona State University (ASU), Tempe, AZ, USA, a Senior Global Futures Scientist with the Global Futures Laboratory and has a joint appointment with the School for the Future of Innovation in Society and the School of Computing and Augmented Intelligence. She was the Founding Chair of the first ever accredited Master of Science degree in Public Interest Technology with ASU and is the Director of the Society Policy Engineering Collective (SPEC). She has worked with OTIS Elevator Company, Minto, NSW, Australia; Andersen Consulting, North Sydney, NSW, Australia; and Nortel Networks, Wollongong, NSW, Australia, from 1994 to 2001. She was the Associate Dean (International) with the Faculty of Engineering and Information Sciences, University of Wollongong, Wollongong.

Roba Abbas received the Ph.D. degree in location-based services regulation from the University of Wollongong, Australia, in 2012.

She has industry experience in Web design and development. She is a Senior Lecturer (Operations and Systems) and an Academic Program Director with the Faculty of Business and Law, University of Wollongong, Wollongong, NSW, Australia, and a Visiting Professor with the School for the Future of Innovation in Society, Arizona State University, Tempe, AZ, USA. She researches methodological approaches to complex socio-technical systems design, emphasizing transdisciplinarity, co-design, and the intersection of society, technology, ethics, and regulation. She has received grants for research addressing global challenges in areas, such as robotics, social media, and other emerging technologies using approaches in socio-technical systems and operations management.

Dr. Abbas is also a Co-Editor of the IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY and the Former Associate Editor of the *IEEE Technology and Society Magazine*. She has appeared on international panels, delivered talks, and co-organized events for Yale University, The Alan Turing Institute, the American Association for the Advancement of Science, and the American Association of Geographers.

Payyazhi Jayashree received the Bachelor of Arts and Master of Arts degrees and the Doctor of Philosophy degree in organizational behavior from the University of Delhi, India, in 1998.

She is the Dean of the Faculty of Business, University of Wollongong Dubai, Dubai, UAE, with core research interests and impact in gender inclusivity for innovation and business transformation. She has led several research teams to achieve the mandate of Leadership, Strategic Change, and Innovation. Her collaborators for these projects include key institutions, such as UN, Dubai Business Women Council, Dubai Chamber of Commerce, and Corporate Leaders and CEOS, from global organizations. Her sustained commitment to UN Sustainable Development Goal#5 and impactful research in Women and Leadership, has led to Global Recognition and substantial Media Coverage, including uptake by prominent scholarly publications, such as *Personnel Review*, and practitioner publications, such as *Forbes* Middle East along with key Awards, such as the "Women of Impact" by UOW, Australia. She is also the Vice President for the Board for Water for People, India Trust, an international nonprofit, based in Denver, working across nine countries to bring safe water and sanitation for four million people.

Ruwan J. Bandara received the B.A. and the Master of Philosophy degrees in organizational management from the University of Peradeniya, Sri Lanka, in 2010 and 2016, respectively, and the Ph.D. degree in business management from the University of Wollongong, Wollongong, NSW, Australia, in 2020. He is an Assistant Professor with the Faculty of Business, University of Wollongong Dubai, Dubai, UAE. He has published in leading international journals, including *International Journal of Information Management*, *Information & Management*, *Journal of Global Information Management*, *International Journal of Operations & Production Management*, *Annals of Operations Research*, *Journal of Business Research*, *European Journal of Marketing*, *Journal of Retailing and Consumer Services*, *Public Administration and Development*, *Journal of International Education in Business*, and *Electronic Markets*. His main research interests focus on responsible business and leadership, future of work, ethical issues of big data and new technologies, and impact of technology on employee/stakeholder wellbeing.

Anas Aloudat (Member, IEEE) received the Bachelor of Science degree in computing from Mu'tah University, Karak, Jordan, in 1993, the Master of Science degree in computing from the University of Technology Sydney, Ultimo, NSW, Australia, in 2003, and the Doctor of Philosophy degree in information systems and technology from the University of Wollongong, Wollongong, NSW, Australia, in 2011.

He was an Associate Professor with Zayed University, Dubai, UAE, from 2018 to 2019, an Associate Professor with the American University in the Emirates, Dubai, from 2016 to 2018, and before that an Assistant Professor of Information Systems and Technology with the Department of Management Information Systems, Faculty of Business, University of Jordan, Amman, Jordan, from 2011 to 2016, and has previously been employed as an Associate Lecturer and a Research Assistant with the University of Wollongong.