Ravida Din and Shoshana Magnet

13 Biometric failure

Abstract: This definition explores how biometric technologies continue to codify a cultural context rife with systemic inequalities.

Keywords: surveillance, security studies, feminist theory, algorithmic bias

Defining biometrics

Biometric technologies render bodies in binary code. Reducing complex and messy material bodies to a series of zeroes and ones—biometric technologies are aimed at making bodies more easily identifiable, speeding the passage of people and commerce. In the words of scholar Katja Franko Aas, biometric and other digital technologies aimed at reading the body "mean that [b]odies become 'coded' and function as 'passwords'" (2006). Biometrics take an electronic reading of the body, an identification process that communication scholars note is at the intersection of multiple communications and information processes, including photography, videography, computer networking, pattern recognition, and digitalization (Gates, 2011). Biometric technologies include, but are not limited to, iris scanning, retinal scanning, digital fingerprinting technologies, and facial recognition technologies. Biometric technologies were originally developed for the prison industrial complex and tested coercively on a population of prisoners that could not refuse to use them. Unsurprisingly, given their beginnings, biometric technologies do not work as claimed for them in ways intimately related to existing inequalities. For example, biometric facial recognition technologies have had and continue to have difficulty reading the bodies of racialized, queer, and disabled people as well as bodies in professions that require a lot of handwashing such as nurses and teachers (Magnet, 2011). In another example, since their onset, retinal scanners have had difficulty identifying the irises of people with dark brown eyes (Magnet, 2011). First used in the prison industrial complex, biometric technologies are now staples of identification in a number of institutions, including state welfare systems, immigration and refugee centers as well as being frequently used in consumer technologies.

How do we define biometric technologies? Definitions are powerful. In Paula Treicher's study of HIV/AIDS, she tells us that there were high stakes involved in naming and definitions within the epidemic, not only for "patent rights to the lucrative test kits for the AIDS virus … but the future and honor of immunology" (1999: 31). So too with biometric technologies. How biometrics are defined concerns not only corporations, policymakers, and consumers, but those who have been forcibly subject to biometric scans in ways intimately connected to what bell hooks called "white suprema-

Acknowledgments: This project is supported by a SSHRC Insight Development Grant # 435 – 2021 – 0035.

 https://doi.org/10.1515/9783111062037-014

cist capitalist heteropatriarchy" (hooks, 1999). Are biometrics a consumer technology that clients may opt-in to in order to facilitate transactions? Are they a requirement of being able to hold a travel document or to get a job? Biometric companies hoping for as many clients as possible have fought to define biometric technologies as an all-purpose, privacy-enhancing solution to the problem of security in the age of insecurity. And yet, so too have biometric technologies been used by privacy and human rights organizations as the case study *par excellence* that reveals the dangers of how technologies can destroy individual and group privacy rights (see Privacy and Data Protection by Bygrave). While "meanings may be multiple, and, even if contradictory, allowed to co-exist in a single space or 'a single head'" (Treichler, 1999), definitions are "less democratic," representing the "outcome of a struggle." How might we complexify the definition of biometric technologies? We argue that a place to start would begin by being attentive to the ways that biometric systems break down or fail.

On failure and biometrics

Failure of biometric technologies to work in the ways claimed for them entrench existing forms of racism, sexism, and ableism as well as homo- and trans- phobias (Magnet, 2011; Browne, 2015). For example, they reliably fail to work distinguishing the faces of people of color (as US and Canadian biometric scanners screening people at the border had difficulty locating the faces of people of color, or had trouble locating the irises of people with dark brown eyes), people with disabilities (as the biometric scanners were too tall for wheelchair users or for little people, but too short for unusually tall people), and queer people (as biometric facial recognition technology is used to split people up into gender categories that rely on assumptions that women have long hair and that only men have short hair and only men wear ties) (Magnet, 2011; Dubrofsky and Magnet, 2015; Hoffer and Savini, 2017; Benjamin, 2019; Weitzberg, 2020). That is, biometric technologies are "haunted" (Gordon, 1997) by histories of white supremacy that assume racialized bodies to be impossibly alike or "haunted" by sexist claims that bodies can speak the "truth" of their gender identities. In other words, biometric technologies are used to perpetuate the myth that the body is no more than "a password" that speaks the truth of its identity (Aas, 2007). (This myth persists despite 100 years of failed attempts to get a lie detector test to work in a reliable fashion; Littlefield, 2009; Cole, 2002). Biometric companies attempt to imagine bodies as stable entities that can give us the definitive proof of identity in ways that permit state actors—including the corporations and governmental departments involved in the prison industrial complex—to surveil and regulate othered communities and populations. And yet, biometric mismatches due to mechanical failures and the technology's inability to work objectively dispute such stability.

Biometric technologies and their attendant failures reveal how we continue to have an impoverished language for thinking more broadly about technological failure. In just one example of this lack, why don't we think of the ways that new technologies

might contribute to the intensification of existing inequalities as failures? For example, biometric technologies rely upon erroneous assumptions about the biological nature of race, gender, and sexuality (Magnet, 2011; Browne, 2010). In so doing they result in bodies that cannot produce a biometric image—whether fingerprint, faceprint, or retinal scan—resulting in individuals who are denied their basic human right to mobility, employment, food, and housing if they cannot be identified by the biometric scanner. Although biometric scientists often speak of 'false accept' or 'false reject' biometric errors, we continue to lack language for thinking about the failures of biometric technologies to contribute to substantive equality. As authors Kaufmann and Vestad remind us, "Criminology has an intimate link to visualization" (2023). So too are the failures of the prison industrial complex intimately bound up with the failures of biometric technologies to visualize the very bodies they claim to be able to codify, as in the case of bodies that simply cannot produce a biometric fingerprint or a reliable retinal scan (Browne, 2010). Moreover, these failures are not simply technical failures, in that biometric technologies are used to visualize crime and criminality in ways that intensify the criminalization and surveillance of racialization from the border to the prison—as well as used to strengthen existing systems of crimmigration—or the criminalization of immigration (van der Woude et al., 2017). As Kaufmann and Vestad argue: "Visual profiles of bodies never emerge out of nowhere. They are a socio-technical practice. They are embedded in the history of explaining crime and the scientization of police and legal work" (Kaufmann and Vestad, 2023).

Biometric technologies are part of the larger problem of technologies that intensify algorithmic bias (Bias by Oswald and Paul), from robotics to search engines to new identification technologies. In the field of algorithmic bias, there is a tendency to think of algorithms as independent entities that are unencumbered by human reflexivity. Algorithms are imagined to hold the promise of objectivity (Daston and Galison, 2007), an objectivity that is perniciously sold to us by large corporations eager to have markets for their technological products. The persistence of "technochauvinism," defined by Meredith Broussard as "a kind of bias that considers computational solutions to be superior to all other solutions" (2023: 2), reminds us how biometric technologies can be sold to consumers as replacing the subjective human eye with the objective gaze of the scanner—failing to think about how the scanner itself codifies existing systemic discrimination.

Artificial Intelligence (AI) encompasses a broad set of algorithms alongside its scaffolding of 'deep learning' and 'machine learning' systems (see Artificial Intelligence by Van Brakel). Central to the operation of these digital technology systems is the availability of massive datasets. According to John Cheney-Lippold, "… one of the primary terms of an algorithm is that everything is represented as data" (2017: 11). It is reasonable, therefore, to assume that algorithms are only as good as the data they are fed, remembering that data is neither made nor collected in a lab sterile to culture. Scholars Safiya Noble (2018), Ruha Benjamin (2019), Wendy Hui Kyong Chun (2021), and Katherine McKittrick (2021) all show that technology is made by human hands—one that are steeped in both a history and a present of white supremacy, of misogyny, of homo-

phobia and of other systemic forms of discrimination. These authors—who are part of larger conversations about algorithmic bias—theorize how historical data, steeped in a broader social context of systemic inequality, leads to discriminatory outcomes that preserve the status quo. For example, describing this reality as the "New Jim Code," Ruha Benjamin argues that this "imagined objectivity reflects and reproduces social hierarchies, whether wittingly or not" (2019: 2) whereas Safiya Noble (2018) describes the ways that search engines encode an existing context of white supremacy as "algorithmic oppression" (p. 17). Furthermore, Joy Buolamwini's groundbreaking work on facial recognition technology too shatters the myth of race as absent from technology when she discovered that the software that she was using failed to recognize her until she donned a white mask. In other words, the machine rendered blackness as illegible, reifying whiteness as its default (Buolamwini and Gebru, 2018). Google's photo-app system, lauded as a pinnacle of human identification, consistently labeled Black people as gorillas. An insidious dehumanization produced through computational 'detachment' is, as Katherine McKittrick explains, "tied to a biocentric system of knowledge" (2021: 111).

Algorithmic bias and complex sorrows

By now, it is well established that algorithmic 'thinking' which produces 'mistakes-to-be-corrected' are not without consequence. The claim that these are simply 'glitches' in the system that require a technical reconfiguration runs contrary to the fact that algorithmic decision-making remains invisible (commonly referred to as the 'black-box' syndrome) to us. Irene Fubara-Manuel (2019) draws on Simone Browne's concept of "critical biometric consciousness" to underscore a praxis of accountability. She writes, "this accountability demands that the architects of these technologies consider the inscriptive practices of biometrics in placing identity on the body. More so, it requires accountability for the ways in which these technologies further subjugation based on race, gender, and disability" (p. 70).

Important to the definition of biometrics is an extension of Marianne Paget's work on mistakes as complex sorrows. Marianne Paget (1993), a sociologist of medicine, argues that "clinical medicine is an error-laden activity" and that we lack words to think about medical mistakes in a complex way. Instead, language taken from legal and insurance discourses about fault and blame dominate our current ways of speaking about medical error; thus, we use the terms *medical malpractice*, *misdiagnosis*, and *negligence*, words that do not get at the affective or emotional nature of medical 'mistakes,' a word seldom used and considered imprecise for the purpose of insurance and legal claims. Biometrics uses the scientific language of 'false acceptance rates' and 'failure to enroll rates' to describe biometric failures. These failures are often understood as exceptional, the result of 'a few bad apples,' rather than as endemic to the science of identification itself. And yet, when biometric scanners are not recognizing the irises of people with dark brown eyes, when retinal scanning technologies are not made acces-

sible to wheelchairs users, and when facial recognition technology disproportionately misrecognizes racialized faces, we know that these errors are endemic to the technologies themselves (Fubara-Manuel, 2019; Magnet, 2011). Given the high stakes of biometric identification, our desire for an error-free science of recognition is great. Yet the desire for error-free biometric technologies does not magic them into existence. Paget refers to medical errors as "complex sorrows" to help us think about both the errors' scientific and emotional implications. Given the devastating consequences of biometric errors for human lives, we need a language that is not restricted to technical terms (see Error by Aradau). Biometric failures as complex sorrows are a beginning.

As I [Shoshana] wrote about in *When Biometrics Fail: Race, Gender and the Technology of Identity* in 2011:

Biometrics became useful as a form of what the security technologist Bruce Schneier (2006) has termed 'security theatre,' or what the border theorist Peter Andreas (2003) calls a 'politically successful policy failure.' Regardless of how often the technologies broke down, worked differentially depending on race and gender, or cost rather than saved the state money, biometrics were used to suggest that *something* was happening. Thus, even when biometric technologies failed, they also succeeded. Whether they were used to assert that the state was getting tough on crime, welfare, or terrorism, biometric technologies were offered up as proof that public–private partnerships were working for the public good, whatever the particular good of the moment might be. Yet despite persistent mechanical failures, biometric technologies still accomplish a great deal for state and commercial actors whose interests are tied to contemporary cultures of security and fear. In this sense biometric technologies succeed even when they fail. On the other hand, even when they function technically, biometrics do real damage to vulnerable people and groups, to the fabric of democracy, and to the possibility of a better understanding of the bodies and identities these technologies are supposedly intended to protect.

And in this sense, and this truth has endured, they fail even when they succeed in reliably identifying bodies with precision. Having detailed the ways that biometric technologies fail in ways intimately connected to systemic oppression—whether they fail to identify the faces of racialized people, whether they are inaccessible for people with disabilities to use at all, or whether they simply fail to work as they are described—we have to remember that they are also an important part of the performative nature of the security industrial complex. That is, biometric technologies continue to make significant profits for the corporations that sell them while suggesting that something by the way of security is indeed happening. Is this the future we want? One of increasingly entrenched technological inequality? Surely not. We need to envision different futures—ones that are not technologically reducible to a series zeroes and ones—but futures concerned with human thriving, with human complexity, and with substantive and intersectional equality. We reduce bodies to binary code at the peril of losing all of the messy complexities that make us truly human.

Suggested reading

Bean, H., & Fischer, M. (2021). Queering intelligence studies. *Intelligence and National Security*, 36(4), 584–598. DOI: https://doi.org/10.1080/02684527.2021.1893078

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness.* Durham, NC: Duke University Press.

Kaufmann, M., & Vestad, M. (2023). Biology and criminology: Data practices and the creation of anatomic and genomic body 'types'. *Critical Criminology*, 31, 1217–1232. https://link.springer.com/article/10.1007/s10612-023-09732-6

References

Aas, K. F. (2006). 'The body does not lie': Identity, risk and trust in technoculture. *Crime, Media, Culture: An International Journal*, 2(2), 143–158. https://doi.org/10.1177/1741659006065401

Benjamin, R. (2019). *Race after Technology: Abolitionist Tools for the New Jim Code.* Cambridge: Polity.

Broussard, M. (2023). *More than a Glitch: Confronting Race, Gender, and Ability Bias in Tech.* Cambridge, MA: The MIT Press. https://doi.org/10.7551/mitpress/14234.001.0001.

Browne, S. (2010). Digital epidermalization: Race, identity and biometrics. *Critical Sociology*, 36(1), 131–150. https://doi.org/10.1177/0896920509347144.

Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness.* Durham, NC: Duke University Press.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1–15.

Chenney-Lippold, J. (2017). *We Are Data: Algorithms and the Making of Our Digital Selves.* New York: NYU Press.

Chun, W. H. K. (2021). *Discriminating Data: Correlation, Neighborhoods, and the New Politics of Recognition.* Cambridge, MA: MIT Press.

Cole, S. A. (2002). *Suspect Identities: A History of Fingerprinting and Criminal Identification.* Cambridge, MA: Harvard University Press.

Daston, L., & Galison, P. (2007). *Objectivity.* Princeton, NJ: Princeton University Press.

Dubrofsky, R., & Magnet, S. (2015). Introduction: Feminist surveillance studies: Critical interventions. In *Feminist Surveillance Studies* (pp. 1–18). Durham, NC: Duke University Press.

Fubara-Manuel, I. (2019). *Animating Opacity: Race, Borders, and Biometric Surveillance.* [Doctoral Thesis, University of Sussex, 2019). http://sro.sussex.ac.uk/.

Gates, K. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* New York: NYU Press.

Gordon, A. (1997). *Ghostly Matters: Haunting and the Sociological Imagination.* Minneapolis: University of Minnesota Press.

Hoffer, K. J., & Savini, G. (2017). Effect of gender and race on ocular biometry. *International Ophthalmology Clinics*, 57(3), 137–142. https://doi.org/10.1097/IIO.0000000000000180.

hooks, b. (1999). *All About Love: New Visions.* New York: William Morrow.

Kaufmann, M., & Vestad, M. (2023). Biology and criminology: Data practices and the creation of anatomic and genomic body 'types'. *Critical Criminology*, 31, 1217–1232. https://link.springer.com/article/10.1007/s10612-023-09732-6

Littlefield, M. (2009). Constructing the organ of deceit: The rhetoric of fMRI and brain fingerprinting in post-9/11 America. *Science, Technology, & Human Values*, 34(3), 365–92. https://doi.org/10.1177/0162243908328756.

Magnet, S. A. (2011). *When Biometrics Fail: Gender, Race, and the Technology of Identity.* Durham, NC: Duke University Press.

McKittrick, K. (2021). *Dear Science and Other Stories.* Durham, NC: Duke University Press.
Nakamura, L., & Chow-White, P. (2013). *Race After the Internet.* New York: Routledge.
Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism.* New York: NYU Press. https://doi.org/10.2307/j.ctt1pwt9w5.
Paget, M. (1993). *Complex Sorrow: Reflections on Cancer and an Abbreviated Life.* Philadelphia: Temple University Press.
Treichler, P. (1999). *How to Have Theory in an Epidemic.* Durham, NC: Duke University Press.
van der Woude, M., Barker, B., & van de Leun, J. (2017). Crimmigration in Europe. *European Journal of Criminology*, 14(1), 3 – 6. https://doi.org/10.1177/1477370816639814
Weitzberg, K. (2020). Biometrics, race making, and white exceptionalism: the controversy over universal fingerprinting in Kenya. *The Journal of African History*, 61(1), 23 – 43. https://doi.org/10.1017/S002185372000002X.