sprinkle: an undergraduate journal of feminist & queer studies | Volume 14 - 2021

Suspicion Encoded: Women of Color and Biometric Technology in the United States

By Lilith Saylor

ABSTRACT. Biometric technology connects the biological and the virtual, informing our physical experience of the world through our virtual data. In this paper, I examine the connection between biometric technology, privacy violations, and US State oppression of vulnerable groups, particularly of poor women of color (WOC) through surveillance and fingerprinting. I argue that poor WOC face intersectional discrimination based on the convergence of sex, race, and class in their identities that renders their inherent right to privacy susceptible to transgression by the State. I highlight the unique and powerful intrusion of biometric technology into the lives of poor WOC and argue that the connection between data and the physical body created through biometric data has formed an environment in which the State wields an unrestricted ability to violate the privacy of poor WOC in both the private and public spheres.

In 2001, Super Bowl XXXV became the site of a massive experiment. As the attendees filed into the stadium in Tampa, Florida, video surveillance monitors scanned the crowds for facial indicators that could match excited football fans to wanted criminals, testing out the Federal Bureau of Investigation's new biometric software and forcing the 100,000 unwitting attendees to participate in a police lineup the size of a small city (Chachere, 2006).

The short-term effects of this experiment located 19 criminals in the crowd, wanted for petty offenses. This experiment confirmed to the Tampa law enforcement agency the long-term benefits of implementing biometric technologies to assist the police. While some citizens praised the surveillance systems set up around Tampa's nightlife district, others, with the support of the Florida American Civil Liberties Union, pointed out that these systems were neither legally regulated nor proven to be accurate (Stanley & Steinhardt, 2002). With the installation of these biometric technologies, many felt more endangered than ever on Tampa's streets.

The following essay explores the commodification of privacy via biometric technology and highlights in particular its impacts on low-income women of color (WOC) in the United States. I expand upon intersectional feminist arguments that WOC face dual discrimination based on sex *and* race to analyze how this manifests in the uniquely intrusive nature of biometric technology for WOC. I argue that the context in which the US utilizes biometric technology reflects a devaluation of working-class women's privacy in the private sphere and a devaluation of POC's privacy in the public sphere, converging to create an environment in which WOC's right to privacy is essentially disregarded.

Gender and the Public/Private Debate

Women, especially those with incomes below the federal poverty threshold, have historically been considered less worthy of privacy than the middle-class heteronormative white man (Allen, 1988; Borgmann, 2009; McClain, 1992; Schneider, 2002). This is evidenced by the intrusive conditions of welfare for mothers and the state's encroachment on the bodily autonomy of women in matters of reproduction, among other invasive state policies.

At the forefront of debates on women's privacy, Anita Allen suggests that the consistent invasion of privacy once occurred because women were "perceived as inferiors, ancillaries, and safe targets" and that many "implicitly assume that daughters, pregnant women, mothers, and wives [were] more accountable for their private conduct than their male counterparts" (Allen, 1999, p. 1178). However, she notes that women have taken great strides towards equality and have gained a more equal standing in the family and the public sphere, thus diminishing the threat of an invasion of privacy in the home. Certainly, Allen is correct in saying that the threat has lessened, but to assume that it has diminished equally for all women is an inaccurate and dangerous conclusion. It is on such a universalizing premise that arguments for privacy protection for women on welfare have all but disappeared, as they were no longer a concern for conventional feminism (Schneider, 2002).

However, issues of privacy for women occur not only in realms in which they lack privacy, but also in those in which they have it. To rationalize its lack of intervention in domestic violence disputes, the state has argued that the family was the arbiter of right and wrong in the home (Schneider, 2002). Thus, women's privacy is only protected in the case that the authority of the heteronormative family surpasses that of the state. While time has improved the nature of women's privacy in domestic violence situations, this development has been uneven due to the fraught relationship communities of color often maintain with law enforcement. For lower-income WOC, the risk attached to calling the police on an abuser, and thus inviting the potential of state retaliation through police violence or nuisance laws, often outweighs the risk of simply accepting the abuse (Kastner, 2015). Thus, even with solid legal developments in the realm of privacy, WOC face unique complications to obtaining privacy across different contexts.

Race and Privacy

Compounding abuses of privacy in the private sphere, WOC face additional discrimination in the public sphere as a result of their race and class status. Warrantless vehicle searches on public roadways constitute a case of an invasion of one's reasonable expectation of privacy assumed in one's vehicle. As stops and searches occur fully at the discretion of state officials, this practice provides legal backing for a state official to disregard a citizen's right to privacy under the nebulous justification of "probable cause." Unlike the bureaucratic and legal frameworks backing a warrant, probable cause implicitly assumes the legitimacy of an officer's situational observations, even if these observations are biased by racial prejudices (Hernández-Murillo & Knowles, 2003). As a result, studies show that POC are significantly

more likely to be searched by the police than white drivers, although white and Black drivers are equally likely to be in possession of contraband (Pierson et al., 2020). Notably, Hispanic drivers were significantly less likely to be in possession of contraband, although they were 4.4-4.6% more likely to be stopped and searched than white drivers (Pierson et al., 2020). Further controls, such as the 'veil of darkness' test comparing stops in the day and the night to ascertain the effect of race on stops and searches, concluded that this disparity was due to racial bias (Grogger & Ridgeway, 2006).

While the scope of this article does not include a discussion on the privacy rights of undocumented immigrants, the treatment of Latinx people during immigration raids represents another state-backed violation of privacy rights in the public and private spheres. These violations of privacy are legally justified on the basis that their intended targets are not citizens and thus do not hold the same rights as citizens; however, the effects of these raids are not limited to non-citizens. Immigration raids, even workplace raids that successfully detain *only* undocumented immigrants, still have the potential to intersect the the private life of legal citizens in mixed-status families by giving officials probable cause to conduct home raids on the families of the detained (Aldana, 2007). Under *INS v. Lopez-Mendoza* (1984), these raids require neither a warrant nor a means of legal entry into the home (Hing, 2009). Further, many of these raids frequently detain citizens on the suspicion that their documents are fraudulent, sometimes holding citizens for weeks without justification (Stevens, 2010; Robertson, 2012; Murray, 2013). Not only do these searches constitute an unconstitutional invasion of privacy, but they also represent the tangible threat that the Latinx community faces when the state allows bias to be coded into law.

Biometric Technology in Welfare

Biometric technologies are those which use and store data on a person's biological measurements in order to establish matches between members of the population and templates in its database. This can include facial recognition software, digital fingerprint databases, retinal scanning technology, and a number of other biological measurements that can be used to identify an individual.

Biometric technology is tied strongly to security in the United States, and the state thus allows it to take liberties with individual rights that other technologies cannot (Kruger et al., 2008). Welfare in the U.S. uses biometrics in an attempt to prevent "double-dipping" fraud, in which welfare recipients apply under multiple identities to receive benefits multiple times. These technologies used digital fingerprinting to identify and track recipients' information and assure that they do not receive the same benefits twice. This technological addition to the bureaucratic arsenal was a product of the Quality Control welfare movement of the 1960s, in which the federal government attempted to shift the responsibility of welfare to the states and capitalized on the growing national unrest around welfare (Magnet, 2011).

It was during this period that the image of the "welfare queen" proliferated as a so-called lazy woman of color with numerous children she could not support from multiple fathers, abusing the system and cheating the "good" American middle class from their hard-earned tax dollars (Gilliam, 1999; Hancock, 2003; Gilman, 2013). The "welfare queen" played on a number of racist fears about the poor Black matriarch. To the white middle class, she was the source of the degeneracy of America, who not only cheated the system for benefits without contributing to the economy but also disrupted the traditional family structure with her moral degeneracy and promiscuity (Hancock, 2003). At the urging of lawmakers, the middle and working classes redirected their frustrations with declining wages, high taxes, and low national production to this stereotype (Reese, 2005). To politicians who invoked the public image of the "welfare queen" to garner support for punitive reforms of welfare, this stereotype was a justification for political intervention into the private lives of the poor (Foster, 2008). Whether all mothers on welfare fit the racial and moral depiction of the "welfare queen" was unimportant; punitive reforms were still targeted at this stereotype and the women who looked the part (Magnet, 2011). In the political realm of welfare, all recipients were encompassed within her image (Hancock, 2003).

As a result of this national mindset set in opposition to welfare recipients, states held the popular support necessary to begin implementing biometric fingerprinting programs to their welfare systems with price tags in the tens of millions. California, the first state to implement this technology, spent $31 million in start-up costs and $11.4 million in yearly maintenance, only to find that the majority of the 11 cases of fraud that it had caught in its first year were the result of administrative errors (Magnet, 2011). With this cost-benefit analysis in mind, one might wonder to what end this and similar programs had been implemented.

Although biometric technologies failed to find significant instances of fraud, the stigma around fingerprinting and the invasive requirements of welfare registration significantly decreased the number of applicants for welfare (Magnet, 2011). Fingerprinting connected to criminality in the public mindset, and the merging of welfare offices and personnel for fraud and standard administration perpetuated this belief of welfare recipients as criminals (Gustafson, 2009). These fingerprints, as a part of a government database, were shared with law enforcement along with extensive personal information including one's home address and the personal information of other family members in order to create hierarchies of need for those seeking benefits (Eubanks, 2018).

For women on welfare, the state's simple demand for access to the fingerprints came with many implications. First, a woman applying for her children must also provide her children's fingerprints (Magnet, 2011). She thus not only connected her own information to law enforcement databases but also her children's information. Second, the lack of privacy within this process placed members of mixed-status families at risk, causing many women to forego seeking benefits so as not to risk personal or family deportation (Xu & Brabeck, 2012). Search provisions allowing welfare officials to enter one's home without notice also

presented an obstacle to women who may have felt unsafe in a private space with a stranger.

One might wonder at the purpose of biometric technology in this setting, as the state could simply enact punitive welfare reforms without this technology and obtain the same outcome. To this, Erin Kruger et al. posits the following:

> In requiring welfare recipients to be biometrically fingerprinted, those who refuse to be biometrically identified are no longer eligible to receive basic sustenance - neither enough food nor a place to live. As such, they are placed outside of law and abandoned" (Kruger et al., 2008, p. 4).

Biometric technology allows the state to withhold basic human rights to those who refuse to be biometrically identified, justifying that the government gave a simple request for fingerprints and was still denied. To those who fail to see the underlying implications of biometric fingerprinting, such a justification may even seem sensible.

Biometric Technology in Surveillance

The advent of the September 11 attacks marked an immense change in the security agenda of the United States. With the founding of the Department of Homeland Security (DHS) in response to the attacks, funding for new securitization technologies gained institutional traction in the US. Whereas the example of mass surveillance in our introduction was met with widespread public debate ,in March 2001 a survey conducted after 9/11 showed that 63% of the adults surveyed supported increased surveillance, and 86% were in favor of facial recognition software to recognize terrorists and criminals (Nieto et al., 2002). It is during this period that biometric and surveillance technologies were rapidly diffused to both state and private agencies, strengthening the flow of data between these bodies (Nieto et al., 2002).

This high level of information sharing has special implications for rising facial recognition software companies. For example, Clearview AI is a private facial recognition provider that supports the largest library of 3 billion facial images for use in computer vision applications. These images were obtained from social media websites without permission and, in some cases, after explicit rejection (Hill, 2020). This company is used by over 600 police departments and the Federal Bureau of Investigation although the National Institute of Standards and Technology has given facial recognition software poor accuracy ratings. Still, the number of police departments using computer vision technology still grows and in many states provides evidence that is admissible in court.

The usage of Clearview AI by law enforcement is not inherently problematic. However, certain elements of this partnership, including its lack of regulation and questionable data collection methods, problematize facial recognition technologies. In particular, facial recognition technologies have displayed different levels of accuracy depending on the race and gender of their subject (Gates, 2015). A study by the National Institution of Science and Technology found that, across the board, Black men and women

were the most likely to be misidentified by facial recognition software by a factor of 10 to 100, depending on the software (Grother et al., 2019). Black women were the most likely to be misidentified, and in one-to-many matches, the type of match that is used to identify persons of interest, they were the most likely demographic to turn out a false positive (Grother et al., 2019). That is to say, Black women were the most likely demographic to be falsely accused of a crime.

Databases like Clearview AI and police databases also represent Black men and women far more than any other demographic as these datasets are also composed of mugshots. This means that for mugshot databases alone, Black men and women are represented 5 times more than white men and women, as this is the proportion at which they are arrested(NAACP, n.d.). In particular, Black women are arrested, and thus represented in mugshots, twice as much as white women. Clearview AI also obtains data by way of individual submissions to the database by police (Hill, 2020). Consequently, any racial bias existing in the criminal justice system is perpetuated in facial recognition technologies used by the state.

Black women face the dual crisis of too much representation and not enough, which manifests in increased arrests and false accusations by biometric findings that are admissible in court. Because Black women lack privacy in the public sphere, they are overrepresented in databases used for apprehending criminals. They are underrepresented in the creation of these technologies, and thus they are more likely to suffer as a result of inaccuracies.

Conclusion

The theory of the "virtual body," forwarded by Irma van der Ploeg, is based on the concept of the informatization of the body through virtual data collection (Van der Ploeg, 2003). The virtual body theory is a critical approach to the claim that the body and its data are separate entities. She argues, "To say that the use of body data merely involves the data or the information, and not the body, or the embodied person themselves, denies the constitutive and enduring relation between the data and my identity as an embodied person" (Van der Ploeg, 2003, p.70). She further argues that as a result of this tangible connection between data and body, it is important that policymakers treat bodily information as worthy of protection, as the extent to which the information is protected reflects the embodied experiences of the individual.

The necessary physical elements of biometric technology complete this connection, as the body itself is the source of identifying information which is then translated into virtual information used to make decisions for the physical body. In the case of welfare, one's virtual information is used to rank the need of welfare applicants, meaning that the ability of a family to exchange personal information for basic necessities affects the resources the state offers them. Families that cannot offer this virtual medium of exchange are placed outside the system and left to fend for themselves, which has consequences on the body in the form of physical and mental stress, hunger, and physical strain following an

over-extended workday. Thus, the consequences of this practice in which the state commodifies information as a bargaining chip for access to human rights are written into a woman's bodily experience. The state's use of biometric technology thus represents the physical, harmful form of unprotected privacy, and WOC must embody these experiences constantly, both privately and publicly.

As a result of their position within intersecting demographics, WOC who apply for welfare benefits are often left by the wayside in discussions of policies and regulations. As situations improve for members of mainstream demographics, WOC disappear from the conversation. However, privacy itself is a deeply intersectional discussion with tangible, physical manifestations in the real world. As biometrics policies develop and become more central to the national dialogue, it is important that we consider the ways that we codify our bias, both into technology and into law.

Lilith Saylor is passionate about the intersection of technology and social justice, particularly as it relates to economic equality and rural development. She recently graduated from Goucher College in Baltimore, MD with degrees in economics, political science, and international relations. She hopes to return to school to pursue graduate studies in a field that will allow her to combine her passions and conduct research exploring the dangers behind rapid, unregulated technological development.

References

Aldana, R. (2007). Of Katz and aliens: Privacy expectations and the immigration raids. *UC Davis L. Rev., 41,* 1081-1136.

Allen, A. L. (1999) Gender and privacy in cyberspace. *Stan. L. Rev. 52,* 1175-1200.

Allen, A. L. (1988) *Uneasy access: Privacy for women in a free society.* Rowman & Littlefield.

Borgmann, C. E. (2009). Abortion, the Undue Burden Standard, and the Evisceration of Women's Privacy. *Wm. & Mary J. Women & L., 16,* 291-325.

Chachere, V. (7 Jan 2006): Biometrics Used to Detect Criminals at Super Bowl. *ABC News*.

Pierson, E., Simoiu, C., Overgoor, J., Corbett-Davies, S., Jenson, D., Shoemaker, A., ... & Goel, S. (2020). A large-scale analysis of racial disparities in police stops across the United States. *Nature human behaviour, 4*(7), 736-745.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* St. Martin's Press.

Foster, C. H. (2008). The Welfare Queen: Race, Gender, Class, and Public Opinion. *Race, Gender & Class,* 162-179.

Gates, K. (2015). Can Computers Be Racist?. *Juniata Voices, 15,* 5-17.

Gilliam, Frank D. (1999). The "Welfare Queen" Experiment: How Viewers React to Images of African-American Mothers on Welfare." *Nieman Reports, 53*(2), 49-52.

Gilman, M. E. (2013). The Return of the Welfare Queen. *Am. UJ Gender Soc. Pol'y & L., 22*, 247-79.

Grogger, J., & Ridgeway, G. (2006). Testing for Racial Profiling in Traffic Stops from behind a Veil of Darkness. *Journal of the American Statistical Association, 101*(475), 878-887.

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test (FVRT): Part 3, Demographic Effects.* National Institute of Standards and Technology.

Gustafson, K. (2008). The Criminalization of Poverty. *J. Crim. L. & Criminology,* 99, 643-716.

Hernández-Murillo, R., & Knowles, J. (2003). Racial Profiling or Racist Policing?: Testing in Aggregated Data. *documento de trabajo, 18*, 1-36*.*

Hill, K. (18 Jan 2020): "The Secretive Company That Might End Privacy as We Know It." *The New York Times*.

Hing, B. O. (2009). Institutional Racism, ICE Raids, and Immigration Reform. *USFL Rev., 44,* 307-52.

INS v. Lopez-Mendoza, 83-491 (US Sup. Ct. 1984). https://caselaw.findlaw.com/us-supreme-court/468/1032.html

Kastner, A. (2015). The Other War at Home: Chronic Nuisance Laws and the Revictimization of Survivors of Domestic Violence. *Calif. L. Rev.,* 103, 1047-80.

Kruger, E., Magnet, S., & Van Loon, J. (2008). Biometric Revisions of the Body in Airports and US Welfare Reform. *Body & Society, 14*(2), 99-121.

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

McClain, L. C. (1992). "The Poverty of Privacy." *Colum. J. Gender & L, 3,* 119.

Murray-Tjan, Laura. (2013). When Will We Stop Deporting US Citizens?. *SSRN 2328697*

NAACP. (n.d.). Criminal Justice Fact Sheet, http://www.naacp.org/pages/criminal-justice-fact-sheet.

Nieto, M., Johnston-Dodds, K., & Simmons, C. W. (2002). *Public and Private Applications of Video Surveillance and Biometric Technologies* (Vol. 2, No. 6). Sacramento: California State Library, California Research Bureau.

Reese, E. (2005). *Backlash against Welfare Mothers: Past and Present.* Univ of California Press.

Robertson, R. (2012). The Right to Court-Appointed Counsel in Removal Proceedings: An End to Wrongful Detention and Deportation of US Citizens. *Scholar, 15,* 567.

Schneider, E. M. (2002). The Synergy of Equality and Privacy in Women's Rights. *U. Chi. Legal F.*, *2002*(1) 137-54.

Stanley, J., & Steinhardt, B. (2002). Drawing a blank: The failure of Facial Recognition Technology in Tampa, Florida. *An ACLU Special Report.* http://www.aclu. org/issues/privacy/drawing_ blank. pdf, 1.

Van der Ploeg, I. (2003). Biometrics and the Body as Information. *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination,* 57-73.

Xu, Q., & Brabeck, K. (2012). Service Utilization for LatinoChildren in Mixed-Status Families. *Social Work Research, 36*(3), 209-221.