January 12, 2022
Dr. Eric S. Lander
Office of Science and Technology Policy
Eisenhower Executive Office Building
Washington, DC 20502

Re: Document No: 2021-21975; Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies

Dear Director Lander,

The National Fair Housing Alliance submits these comments in response to the Office of Science and Technology Policy's ("OSTP") Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.[1] We applaud the OSTP for seeking input on this important topic and believe the responses below will provide fair housing and lending context for public and private sector biometric technologies. We hope our feedback will help inform the OSTP's policies to address consumer consent, privacy, racial targeting, racial profiling, and other implications of biometric technologies.

I. Summary:

We first address how biometric information is being used to identify people and make inferences them in algorithmic systems like credit scoring, facial recognition technologies, and tenant screening tools. Biometric systems are increasingly being used in the banking, financial services, and insurance (BFSI) industries. The increased usage of biometric information for banking authentication, sign-in applications, customer identification, security, and other applications, raises privacy, discrimination, and consumer consent concerns. The usage of biometric data in such cases may be used to monitor and further marginalize communities of color, women, and other underserved groups and can result in the denial of housing or lending services, identity theft, or higher premiums for homeowners' insurance.

We then go on to address security considerations associated with a particular biometric technology in the context of privacy. Massive data breaches linked to biometric data have already occurred and the potential for criminal activity and fraud, specifically identity theft, is increased after a breach. Leakage of personal data connected to an individual's biometric data can cause irreversible damage such as compromising a credit score to the extent where it is difficult for individuals to secure mortgage loans. For people of color who disproportionately have thin credit files or are credit unscorable, cybercrime due to biometric data breaches may make them vulnerable to privacy risks that prevent them from passing through the early screening stages of a credit application.

Lastly, we address the exhibited and potential harm of facial recognition. Facial recognition is used by law enforcement for surveillance which is concerning considering disparities in error rates across different demographic groups with the least consistent accuracy

[1] National Archives. (2021, October 8). *Notice of request for information (RFI) on public and private sector uses of biometric technologies.* Federal Register. Retrieved January 15, 2022, from https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

found for Black females.[2] Facial recognition for surveillance has a high correlation to insecure housing, loss of employment opportunities, and increased criminalization of surveilled people.[3] Facial recognition for surveillance is also occurring in the housing sector, including in housing owned or supported by funding from the Department of Housing and Urban Development (HUD). Responsible monitoring and oversight over the use of biometric data in the housing space is rare and ineffective. For example, HUD does not monitor the use of this highly sensitive data for the approximately 1.2 million households living in public housing. Nor does HUD carry out research or provide policy guidance for the use of biometric data and instead leaves those most vulnerable in our society to deal with the repercussions.[4] Additionally, the ramifications of false to trivial criminal allegation due to errors in facial recognition loss of access to government relief programs, and other harmful consequences, thus exacerbating existing inequalities through more difficult access to housing and lending opportunities and elevated privacy concerns. .

II. Background:

Biometrics is the automated recognition of people based on the analysis and measurement of their unique physical and/or behavioral attributes.[5] The two main types of biometric identifiers are physiological characteristics and behavioral characteristics. Physiological identifiers derive from structural information of the human body and include the following: facial features, fingerprints, finger geometry (the size and position of fingers), iris, veins, retina, voice, and DNA (deoxyribonucleic acid).[6] Behavioral identifiers include the unique ways in which individuals act, including recognition of typing patterns, mouse and finger movements, social media engagement patterns, walking gait, and other gestures[7]. Biometric technology is being used in sectors such as housing, BFSI, government, defense, and security, and is poised to enter even more sectors.[8] Biometric systems have been deployed in a variety of applications like mobile phones, consumer banking authentication, housing security systems, international border crossing, and national ID programs.[9]

Limitations to implementing biometrics-based systems include cost considerations but the major concerns are the possibility of bias, security breaches, and error rates.[10] As biometric systems become more integrated into society, there must be an effort to increase public understanding of how biometric data is gathered, used, and stored, as well as how it can be

---

[2] Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face recognition performance: Role of demographic information. IEEE Transactions on Information Forensics and Security, 7(6), 1789-1801.

[3] Urban, N., Yesh-Brochstein, J., Raleigh, E., & Petty, T. (2019, June 9). A Critical Summary of Detroit's Project Green Light and its Greater Context.

[4] Ng, A. (2020, June 22). *US government doesn't know how it uses facial recognition in public housing.* CNET. Retrieved January 13, 2022, from https://www.cnet.com/news/us-government-doesnt-know-how-it-uses-facial-recognition-in-public-housing/

[5] Kloppenburg, S., & Van der Ploeg, I. (2020). Securing identities: Biometric technologies and the enactment of human bodily differences. *Science as Culture,* 29(1), 57-76.

[6] Gillis, A. S., Loshin, P., & Cobb, M. (2021, July 26). *What is biometrics*? Search Security. Retrieved January 13, 2022, from https://www.techtarget.com/searchsecurity/definition/biometrics

[7] Ibid.

[8] Sonawane, K. (2016, June). *Biometric technology market size, share and Industry Forecast - 2022.* Allied Market Research. Retrieved January 11, 2022, from https://www.alliedmarketresearch.com/biometric-technology-market#:~:text=Owing%20to%20its%20unique%20characteristics,gaming%2C%20automobile%2C%20retail)

[9] Thales Group. (2021, June 2). *Biometrics: Definition, use cases, latest news.* Thales Group. Retrieved January 15, 2022, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics J

[10] Ibid.

weaponized against consumers, particularly consumers of color.[11] There must also be increased efforts to regulate how this data and systems built using it are regulated.

III. Descriptions of Use of Biometric Technology for Recognition and Inference:

Biometric technology is being used in sectors such as housing, banking, finance, government, defense, and security.[12] In fact, the global biometric technology market is experiencing exponential growth with some researchers projecting that the biometric technology market will reach $86.61 billion by 2027.[13] As current uses are expanded and more applications are created, the potential for harm to people and unintended consequences increases.

The BFSI industry is turning to biometric technology more and more to reduce risks, identify users, track consumer activity, and keep consumers satisfied by increasing the speed of banking authentication and transactions. Entities like Bank of America, Chase and PNC have given their customers the ability to save their fingerprints or face on smart devices.[14] Lenders are using biometrics to verify identities in a virtual environment where in-person loan closings are rare. Companies are also using this data to detect and mitigate fraud.

Although fingerprint authentication has its benefits, one problem it presents is that it can open the door for familiar fraud which may hurt consumers' capacity to access credit. Familiar fraud is a form of identity theft that is caused by someone familiar to a person, like a family member or friend. It is thought to be under-reported because victims may not want to strain family bonds, or they may believe that authorities may not believe them. Additionally, it may take years before someone realizes they were a victim of familiar fraud.

Axton Betz-Hamilton was one such person. In 2013, Ms. Betz-Hamiliton unearthed a credit report that was taken out by someone who had been stealing her identity since she was 11 years old.[15] She also unearthed a file containing incriminating documents and that is when she realized that the person who had destroyed her life and put her father and grandfather into debt was her now-dead mother. Her mother had "stolen" half a million dollars while Ms. Betz-Hamiliton was left with a 380-credit score, pages upon pages of fraudulent credit-card charges, and collection-agency entries in her name.[16] With a 380-credit score Ms. Betz-Hamiliton may have been faced with high premiums for auto and homeowners' coverage, difficulty renting or buying a home, and difficulty financing other major purchases.

---

[11] Millett LI, & Pato JN. (2010, January 1). *Cultural, social, and legal considerations.* Biometric Recognition: Challenges and Opportunities. Retrieved January 10, 2022, from https://www.ncbi.nlm.nih.gov/books/NBK219893/

[12] Sonawane, K. (2016, June). *Biometric technology market size, share and Industry Forecast - 2022*. Allied Market Research. Retrieved January 11, 2022, from https://www.alliedmarketresearch.com/biometric-technology-market#:~:text=Owing%20to%20its%20unique%20characteristics,gaming%2C%20automobile%2C%20retail)

[13] MarketWatch. (2022, January 7). *Contactless biometrics technology market scope and Overview, estimates & forecast, by application, segments* 2022?2030. MarketWatch. Retrieved January 11, 2022, from https://www.marketwatch.com/press-release/contactless-biometrics-technology-market-scope-and-overview-estimates-forecast-by-application-segments-20222030-2022-01-07?tesla=y

[14] Lee, J. (2016.). *Banks turn to biometrics to boost security*. NerdWallet. Retrieved January 11, 2022, from https://www.nerdwallet.com/article/banking/biometrics-when-your-bank-scans-your-voice-face-or-eyes

[15] Thernstrom, M. (2019, October 15). *What if the thief who steals your identity is your mom?* The New York Times. Retrieved January 11, 2022, from https://www.nytimes.com/2019/10/15/books/review/the-less-people-know-about-us-axton-betz-hamilton.html

[16] Cohen, S. (2019, October 12). *I lived with the identity thief who ruined my family - and didn't realize until it was too late.* New York Post. Retrieved January 15, 2022, from https://nypost.com/2019/10/12/i-lived-with-the-identity-thief-who-ruined-my-family-and-didnt-realize-until-it-was-too-late/

If this tragedy had occurred during modern times, when companies are relying on biometrics, it is possible the damage to Ms. Betz-Hamilton could have been much worse. In order to establish a false identity, a false doppelganger, Ms. Betz-Hamilton's mother would have had to use her own biometric information to establish an identity for the pseudo Ms. Betz-Hamilton. How would the real Betz-Hamilton ever be able to verify her true identity using her real biometric information when a false identity had already been established for her using her mother's biometric information? Use of biometrics technologies raises serious privacy concerns. Wherever an individual goes, they leave behind biometric information. Fingerprints can be left behind when a person touches an object. A voice can easily be recorded by home devices such as Google Home and Alexa even when not prompted. An individual's image can be taken at any time, even without their knowledge. Not only that, but highly skilled thieves can easily replicate biometrics information such as fingerprints. This becomes worrying especially now that biometric technologies, like facial recognition, are being used by agencies such as the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), U.S Customs and Border Protection (CPB), and police departments like the New York, Chicago, and Detroit Police Departments. These agencies utilize biometric technologies without the consent of individuals which may heighten privacy concerns. In the U.S, surveillance is concentrated among racial and ethnic minorities, particularly - Black and Latino men.[17]

Landlords could use biometric information to discriminate against protected classes. There are no regulations to stop a landlord from denying a prospective tenant just because they do not meet a certain biometric threshold. A landlord may rely on information from a tenant screening selection vendor that utilizes criminal records information to assess potential tenants.[18] This poses potential discrimination challenges since many law enforcement departments utilize facial recognition technology that is notoriously biased toward people of color resulting in higher instances of false identifications and wrongful arrests for this group.[19] The challenge is that tenant screening selection systems can ding a potential tenant just for being arrested – even if the arrest was unjustified.[20] In situations like this, biometrics can form the basis for discriminatory outcomes in a housing context and lead to the disenfranchisement of Black and Brown consumers and the restriction of their ability to fairly access critical housing opportunities.

The hyper-policing of communities of color, which is exacerbated by facial recognition and other biometrics technologies, results in Blacks and Latinos being disproportionately arrested. This biometrics-based data is then fed into systems used in the housing sector, like tenant screening selection technologies, that result in people of color being disproportionately excluded from housing opportunities. This process can reinforce and perpetuate segregation

---

[17] Remster, B., & Kramer, R. (2018). Race, space, and surveillance: Understanding the relationship between criminal justice contact and institutional involvement. *Socius, 4*, 2378023118761434.

[18] See Shannon Houston, *Center Files Federal Lawsuit Against National Tenant Screening Company*, Connecticut Fair Housing Center, (August 24, 2018). In this case, a mother was denied the right to have her disabled son live with her because the apartment complex where she lived used a tenant screening selection service that flagged the son because he had been arrested as a minor. He was never convicted of committing any crime.

[19] Alfred Ng, *Police are Using Facial Recognition for Minor Crimes Because They Can*, CNET, (October 24, 2020).

[20] Cyrus Farivar, *Tenant Screening Software Faces National Reckoning*, NBC News (March 14, 2021). https://www.nbcnews.com/tech/tech-news/tenant-screening-software-faces-national-reckoning-n1260975

and also lead to "biometric redlining" that prevents Black and Brown individuals from accessing housing opportunities in predominantly White, resource-rich neighborhoods.

When it comes to the gathering of biometric information such as facial images, eye scans, and vocal data , individuals often do not have meaningful ways to opt out of the collection of their personal information. In Knickerbocker Village, an affordable housing complex located in New York City, tenants were required to submit to facial scanning. Tenants' facial scans are assessed by a facial recognition system that tenants, who are predominantly Chinese, complain rarely works.[21] Children as young as 8 years old have had to submit to facial scans and must submit to several more scans as they grow older.

Regulation over the use of facial recognition systems is quite lax. For example, Knickerbocker Village did not submit the necessary application to gain approval from New York's Division of Housing and Community Renewal for use of the facial recognition system.[22] For years, the housing complex has allegedly been illegally using facial recognition technology. Weak regulation and oversight have prompted legislators to take note. Representatives Yvette Clarke, Ayanna Pressley, and Rashida Talib introduced the No Biometric Barriers Housing Act of 2019.[23] It is not clear how companies like Knickerbocker Village use the biometrics data collected in its facial recognition system. While the complex alleges it is only using the data and systems for safety purposes, they create clear barriers for the residents of the community and could be used for surveillance, rather than safety purposes.

Some entities are utilizing biometrics without the consent or knowledge of their target group.[24] Clearview AI created a facial recognition application that was built from more than 3 billion images scraped from websites such as Facebook, YouTube, Venmo, and millions of other websites. This application allows companies to take a picture of a person, upload the image into the application and get public photos of the target with links to the website where the photo was posted. This application infringes on the privacy rights of individuals. There are no regulations preventing a potential landlord from taking a photo of prospective tenants and selling that data to a company like Clearview. Nor are there regulations that would prevent landlords from sending images of tenants' driver's licenses or passports to a company like Clearview.

Systems like those created by Clearview could also be used by potential employers, car lenders, and other entities to discriminate based on biometric data. Given the lax regulatory oversight over these types of utilities, it is difficult to fully understand the full potential for discrimination they can manifest. In housing and lending, applications like Clearview can be used to monitor and cause biometric redlining by denying those deemed "high risk" from renting an apartment or receiving a credit card. Biometric redlining can also be exacerbated by a type of biometric technology that was suggested by PayPal's global head of developer evangelism, Jonathan LeBlanc. LeBlanc suggested replacing traditional biometrics like

---

[21] Kim, E. (2019, September 18). *'we're like guinea pigs': How an affordable Lower East Side Complex got facial recognition*. Gothamist. Retrieved January 11, 2022, from https://gothamist.com/news/were-guinea-pigs-how-affordable-lower-east-side-complex-got-facial-recognition

[22] Ibid.

[23] See Press Release *Reps. Clarke, Pressley & Tlaib Announce Bill to Ban Public Housing Usage of Facial Recognition & Biometric Identification Technology*

[24] Roussi, A. (2020, November 18). *Resisting the rise of facial recognition*. Nature News. Retrieved January 11, 2022, from https://www.nature.com/articles/d41586-020-03188-2

fingerprints and iris scans with invasive systems.[25] One suggestion included a password pill that could be ingested and powered by stomach acid. Other solutions included “tattoos” incorporating a computer chip, embedded wireless antennas, and sensors that measure temperature, ECG activity, etc. These technologies could be used to track and over police communities of color which infringes on individual rights and these communities‘ right to privacy.

Biometric applications, like the one developed by Clearview, bring up data ownership and personal privacy problems. These applications can also be weaponized against Black and Latino communities and those that oppose powerful organizations. In the future, applications like Clearview can be used by governments to stop civil protests, stalk political opponents for blackmailable information, monitor already disenfranchised communities and so much more.

IV. Security Considerations Associated With A Particular Biometric Technology:

The importance of right to Privacy cannot go unnoticed as technology increases its hold on every facet of the human experience. The misuse of or unauthorized access to biometric data can compromise privacy and could have serious long-lasting implications. While exposure to biometric technology increases and persists in shaping individuals' interactions online, it is important to address real issues of how biometric technologies can enable privacy and integrity attacks in a way never seen before.

Biometric authentication utilizes either human physical or behavioral characteristics to identify an individual and provide access to systems’ data or devices. Biometric characteristics serve as identifiers to authenticate or, in partnership with other means of information, to identify a user. Such private information is progressively collected, stored, and transmitted by IoT (Internet of Things) devices and services in the Cloud thus making individuals more vulnerable to cyberthefts.[26] Biometric data is easier to hack than other types of data and the implications of misusage may be incredibly dangerous.[27] Though there are safer ways to store biometric data such as through chips or end-user devices like smartphones, a biometric server is the most cost-efficient way to store such data.[28] However, data in a biometric server is more susceptible to access breach compared to other types of data, despite allowing for verification in multiple locations, due to how biometric technology— unlike encryption keys and codes— captures a single unique identity that is immutable.[29] The static state of biometric data makes it more prone to identity-based threats. Therefore, through access to biometric data either through data breach or misusage, hackers or other parties can easily steal identities or even tamper with and use such biometric information to the detriment of an individual.

---

[25] Collins, K. (2015, April 20). *PayPal wants you to swallow your password.* WIRED UK. Retrieved January 11, 2022, from https://www.wired.co.uk/article/paypal-biometric-security-edible-passwords-tattoos

[26] Haber, M. (2019, March 21). *Is Your Identity at Risk from Biometric Data Collection?.* Beyond Trust. Retrieved January 13, 2022, from https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection

[27] Porr, P. (2020, April 13). *The Fear of Biometric Technology in Today's Digital World. CPO Magazine.* Retrieved January 13, 2022, from https://www.cpomagazine.com/data-privacy/the-fear-of-biometric-technology-in-todays-digital-world/

[28] Ibid.

[29] Johansen, A. G. (2019, February 8). *Biometrics and Biometric Data: What is it and is it Secure?* Norton. Retrieved January 13, 2022, from https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html

Spoofed sensors[30], sensor inaccuracy, host system misconfigurations, and additional fraud capabilities can imperil biometric indicators. Such happened when the U.S. Office of Personnel Management was hacked in 2015 and cybercriminals got access to 5.6 million government employees' fingerprints leaving them vulnerable to identity theft.[31] Then in 2019 a major breach was found in the biometric system utilized by UK Police, defense contractors, and banks.[32] A million people's fingerprints, log data, facial recognition, and additional personal information were compromised and found on a publicly accessible database. Biometric characteristics are immutable and, once stolen, resulting negative consequences may be irreversible. This puts individuals at risk of being affected for the rest of their lives.

The potential for criminal activity and fraud, specifically identify theft, is massive. Leakage of personal data connected to an individual's biometric information can cause irreversible damage such as compromising a credit score to the extent that it makes it difficult for individuals to secure housing, mortgage loans, and other financial services. The types of identity theft that directly impact the purchase of a home include tax identity theft, Social Security identity theft, financial identity theft, and medical identity theft.[33] These types of identity theft will affect an individual's credit score due to how such cybercrime results in unpaid bills, debt from loans, and balances due on credit lines despite being impersonated. Examples of compromised biometric indicators' consequences are endless; thus, it is necessary to address the lack of needed oversight and security to keep biometric data from advanced authentication technology safe.

These complex technical, process, and policy challenges must be addressed to ensure digital data is secured and biometric technology effectively shapes human identity authentication applications for the better.

V. Potential Harms of A Potential Biometric Technology:

Today, an estimated one hundred and thirty countries around the world have data protection laws and almost all these laws cover biometric data protection guidelines.[34] In theory, these laws make sure biometric data is not utilized for instances where customers do not give consent. However, these laws lack attention to racial bias, discrimination, or accuracy, and they are often too complex to faithfully implement in an algorithmic system. Of all dominant biometrics-based technology applications, facial recognition is one of the least accurate and it has a legitimate basis for privacy concerns.[35]

---

[30] A spoof sensor is used in spoofing attack, a situation in which a person or program successfully impersonates another by falsifying data, to gain an illegitimate advantage. See Jindal, K., Dalal, S., Sharma, K. K. (February 2014), Analyzing Spoofing Attacks in Wireless Networks, 2014 Fourth International Conference on Advanced Computing Communication Technologies: 398–402. doi:10.1109/ACCT.2014.46.

[31] Sanger, D. E. (2015, September 23). *Hackers Took Fingerprints of 5.6 million U.S. workers, Government Says.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html

[32] Doffman, Z. (2019, August 14). *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records*. Forbes. Retrieved January 13, 2022, from https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=4523dc1a46c6

[33] National Consumer Law Center. (2021, December). No Silver Bullet: Using Alternative Data for Financial Inclusion and Racial Justice.

[34] Vioreanu, D. (2021, November 15). B*iometric Tech is Here to Stay – Unveiling the Privacy and Security Risks.* Privacy Hub. Retrieved January 13, 2022, from https://privacyhub.cyberghostvpn.com/privacyhub/privacy-concerns-biometrics/

[35] Najibi, A. (2020, October 26). *Racial Discrimination in Face Recognition Technology. Science in the News.* Retrieved January 13, 2022, from https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

Facial recognition's widespread implementation ranges from the ability to unlock a smart phone to law enforcement surveillance to employment and housing decisions. Around half of all adults in America, meaning over 117 million people, have their photos in a facial recognition network used by law enforcement agencies.[36] Law enforcement utilizes the facial recognition network to compare photos of suspects to images of drivers' licenses and mugshots. Such application of facial recognition is taking place largely without awareness, much less individual consent. The widespread implementation of these technologies in a law enforcement context is disturbing, particularly when one considers the pronounced racial bias, especially towards Black people, these systems manifest.[37]

New and growing research reveals puzzling disparities in error rates across different demographic groups with the least consistent accuracy found for 18 to 30-year-old Black females.[38] Additionally, the landmark "Gender Shades" project from 2018 applied an intersectional approach to appraise three different gender classification algorithms including those of Microsoft and IBM.[39] Subjects for the project were put into four categories of darker-skinned females, darker-skinned males, lighter-skinned females, and lighter-skinned males. All three gender classification algorithms performed with the least accuracy on darker-skinned females with error rates that were 34% higher than those for lighter-skinned males.[40] The National Institute of Standards and Technology validated these studies and found facial recognition for 189 algorithms to perform with the least accuracy on women of color.[41]

The research is undeniable, and such harrowing results have led to prompt responses around the conversation of equity in facial recognition. The implications of high error rates in facial recognition systems utilized by law enforcement is troubling due to historical and existing racist patterns of law enforcement which disproportionately hurt the Black community and other marginalized populations. Surveillance through facial recognition technologies by law enforcement threatens important rights such as "privacy, freedom of expression, freedom of association, and due process" as vocalized by the Algorithmic Justice League.[42] Surveillance is could lead to behavioral changes such as self-censorship due to fear of retribution.[43] Fear of retribution due to activism is not unfounded, as facial recognition was utilized to monitor and identify peaceful Black Lives Matter protestors in 2020.[44] Some of the greatest harmful implications of facial recognition technology lies in the criminal justice context where inherently biased facial recognition technologies can misidentify suspects due to the low level of accuracy. This can and has resulted in higher levels of arrest and incarceration of innocent Black

---

[36] Ibid.

[37] Bedoya, A. M. (2020). Privacy as Civil Right. *NML Rev., 50,* 301.

[38] Klare, B. F., Burge, M. J., Klontz, J. C., Bruegge, R. W. V., & Jain, A. K. (2012). Face recognition performance: Role of demographic information. *IEEE Transactions on Information Forensics and Security*, 7(6), 1789-1801.

[39] Buolamwini, J., & Gebru, T. (2018, January). Gender shades: Intersectional accuracy disparities in commercial gender classification. *In Conference on fairness, accountability and transparency* (pp. 77-91). PMLR.

[40] Ibid.

[41] Grother, P. J., Ngan, M. L., & Hanaoka, K. K. (2019). Face recognition vendor test part 3: demographic effects.

[42] *What is Facial Recognition Technology?* Algorithmic Justice League. (n.d.). Retrieved January 13, 2022, from https://www.ajl.org/facial-recognition-technology

[43] Munn, N. (2016, November 8). *How Mass Surveillance Harms Societies And Individuals - And What You Can Do About It.* CJFE. Retrieved January 13, 2022, from https://www.cjfe.org/how_mass_surveillance_harms_societies_and_individuals_and_what_you_can_do_about_it

[44] Choudhury, N., & Cyril, M. (2021, November 19). *The FBI won't hand over its surveillance records on 'black identity extremists,' so we're suing.* American Civil Liberties Union. Retrieved January 13, 2022, from https://www.aclu.org/blog/racial-justice/race-and-criminal-justice/fbi-wont-hand-over-its-surveillance-records-black

Americans thereby worsening America's already damaged, biased and discriminatory criminal justice system..

Facial recognition for surveillance gone wrong was most notably seen in Project Green Light, a 2016 model surveillance program.[45] High-definition cameras were installed in the city of Detroit and the cameras' data directly went to the Detroit PD to test for facial recognition against criminal databases, driver's licenses, and state ID photos to include almost every resident of Michigan in this system without any individual consent.[46] The Project Green Light Cameras were not distributed evenly across the city and instead were concentrated in majority-Black areas whilst excluding majority White and Asian areas.[47] Direct consequences of concentrated Project Green Light Cameras in majority Black areas were revealed through a critical analysis of Project Green Light in 2019. The critical analysis reported such surveillance and data collection had a high correlation to insecure housing, loss of employment opportunities, and the increased criminalization and policing of community members who encountered this model surveillance program.[48]

The criminalization and policing of community members due to the concentration of Project Green Light Cameras in majority-Black areas can have dire impacts including lowered credit ratings, denial of housing and lending opportunities, eviction, and the presence of debilitating information on a person's credit report. This can, of course, reduce a person's ability to rent or buy a home or obtain employment.

If any incarcerated individual has outstanding debt, they are not always able to pay such debt from jail, thus negatively impacting their credit score. Moreover, people who are arrested will undoubtedly have to tap into financial resources to cover legal fees or bonds. This can mean piling up credit card debt or even obtaining PayDay loans and both will have a harmful affect on a person's credit score. First, higher debt utilization lowers a person's credit score. Secondly, accessing PayDay loans, which can often have abusive and predatory terms, can more likely result in outcomes, like increased collections activity, that will harm a consumer's financial profile. Additionally, closing credit cards and extreme periods of inactivity on a card can also hurt credit scores and serve as a barrier for buying or renting houses, obtaining homeowners insurance, and more.

Project Green Light is a striking example of the way surveillance through facial recognition can perpetuate racial inequality when there is no regulation. Tawana Petty, director for the data justice program for the Detroit Community Technology Project and lifelong Detroit resident explained "It feels like digital redlining; that people are being regulated to particular neighborhoods and identified in particular ways because those cameras exist."[49]

Though more lawmakers are beginning to push for regulation, it is hard to do so when there is no documentation for or tracking of surveillance applications especially in the location

[45] Harmon, A. (2019, July 8). *As cameras track Detroit's residents, a debate ensues over racial bias.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html

[46] Urban, N., Yesh-Brochstein, J., Raleigh, E., & Petty, T. (2019, June 9). A Critical Summary of Detroit's Project Green Light and its Greater Context.

[47] Harmon, A. (2019, July 8). *As cameras track Detroit's residents, a debate ensues over racial bias.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html

[48] Urban, N., Yesh-Brochstein, J., Raleigh, E., & Petty, T. (2019, June 9). A Critical Summary of Detroit's Project Green Light and its Greater Context.

[49] Fadulu, L. (2019, September 24). *Facial recognition technology in public housing prompts backlash.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html

Americans spend most of their time, their homes.[50] The Department of Housing and Urban Development (HUD) does not keep track of the way surveillance technology may be used on its 1.2 million households.[51] A letter from HUD to Senator Wyden(OR) stated the agency does not know how many of their public housing programs utilize facial recognition or the way it is allowed to be used.[52] Though these are federally assisted properties under HUD's jurisdiction, rather than monitoring the usage of facial recognition technologies, they leave such responsibilities to individual Housing Authorities that implement housing programs. HUD also never carried out research or implemented policies or guidance for how facial recognition can be used in public housing.[53]

While many multi-family housing corporations assert, they are utilizing systems fueled by biometric data to address safety concerns, there is ample evidence that these systems are being used to conduct surveillance on inhabitants. In the Fall of 2018, tenants at the Atlantic Plaza Towers received a concerning letter in the mail stating their landlord was going to install facial recognition technology to access their building and replace the key-fob system they previously.[54] Not every tenant knew of these changes and five tenants convened in the lobby to spread the word. A couple of days later, those five tenants, who were Black women, received a note from the property management company stating that the lobby was not "a place to solicit, electioneer, hang out, or loiter," along with pictures of them convening.[55] New York State law gives tenants the right to meet peacefully in any location of the building as long as they are not obstructing passageways which the women are not shown to be doing as evidenced by the pictures. [56] It is clear that the property management firm was utilizing the facial recognition system to police tenants and that the company's interpretation of what the tenants were doing was inaccurate.

The ramifications of false or trivial criminal allegation through surveillance by facial recognition carry heavy consequences. Individuals in public housing or the rental market may face civil asset forfeiture, eviction, or loss of access to government benefits and relief programs in the future. Such consequences are already dominant for people of color and women, thus unregulated facial recognition could exacerbate existing structural inequalities in the U.S. impeding access to fair housing, lending, and other opportunities and presenting privacy and due process, consumer consent concerns.[57]

[50] Ng, A. (2020, June 22). *US government doesn't know how it uses facial recognition in public housing.* CNET. Retrieved January 13, 2022, from https://www.cnet.com/news/us-government-doesnt-know-how-it-uses-facial-recognition-in-public-housing/
[51] Ibid.
[52] Ibid.
[53] Fadulu, L. (2019, September 24). *Facial recognition technology in public housing prompts backlash.* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/09/24/us/politics/facial-recognition-technology-housing.html
[54] Bellafante, G. (2019, March 28). T*he landlord wants facial recognition in its rent-stabilized buildings. why?* The New York Times. Retrieved January 13, 2022, from https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html
[55] Ibid.
[56] Ibid.
[57] Ng, A. (2019, July 22). *Lawmakers to introduce Bill to ban facial recognition from public housing.* CNET. Retrieved January 13, 2022, from https://www.cnet.com/home/smart-home/facial-recognition-may-be-banned-from-public-housing-thanks-to-proposed-law/