International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 11, Issue 1 - V11I1-1469)
Available online at: https://www.ijariit.com

Data Privacy and Artificial Intelligence Governance for Marginalized Communities in the United States: How Important is Inclusivity?

Idara Bassey
baseyidara@gmail.com
University of Illinois, Urbana-Champaign, United States

ABSTRACT

The study, "Data Privacy and AI Governance for Marginalized Communities in the United States," examines the digital divide affecting marginalized groups and its exacerbation by biased AI governance. With the objectives of assessing data privacy risks, analyzing biases in AI systems, and proposing inclusive policies to improve AI governance, the research highlights key findings, including that marginalized communities, particularly racial minorities and low-income populations, face disproportionate risks from surveillance capitalism, biased facial recognition, and AI-driven hiring processes. Healthcare is also affected by the technological bias as AI models less accurately serve marginalized groups owing to unrepresentative data sets. In response, the study recommends stringent data protection laws akin to the European Union's GDPR, ethical AI standards focused on transparency, as well as mandatory diversity in AI development teams to ensure demographic representation. To address biases in surveillance, the enactment of the George Floyd Justice in Policing Act and the Facial Recognition and Biometric Technology Moratorium Act are recommended. The work concludes with an emphasis on the need for digital inclusion and equitable AI governance to prevent further marginalization and foster fair participation in a digital society.

Keywords: *Artificial Intelligence Governance, Bias, Digital divide, Data Privacy*

INTRODUCTION

Understanding Marginalization and Digital Divide

Today, having access to technology and the internet has become an essential part of societal life. This impacts everything, from social interaction and education to employment relationships and healthcare. Amidst this, a large number of the United States (U.S.) population remain disconnected from the general public, creating a "digital divide" of marginalized groups consisting of racial and ethnic minorities, low-income households, rural populations, the elderly, and people with physical and mental impairment. Thanks to systemic injustice, and economic hardship, poor infrastructure, these groups often encounter barriers to using digital devices, accessing the internet, and digital literacy tools (Anderson & Perrin, 2018).

Governments, private companies and organizations collecting personal data from civilians is another practice that has become common place today. These data collectors use "national security", "economic stability", or "other societal benefits" as justifications when the privacy of the data subjects is compromised. The trade-offs do not impact all individuals proportionately. Ironically, communities of color in the U.S. under both past and current political regimes have been diversely impacted by data collection and surveillance (Turner-Lee & Chin-Rothmann, 2022). This is generally termed marginalization.

Marginalization, otherwise termed 'social exclusion', occurs when an individual or group of individuals are largely incapable of doing or accessing certain opportunities, general rights or basic services (Civil Liberties Union for Europe, 2021) It is the treatment of a person, group, or concept as insignificant or merely incidental. It can be added that marginalization is the social and economic isolation of certain groups from mainstream opportunities, which results in limited access to resources and opportunities that others may take for granted.

Historically marginalized communities in the U.S. have been faced with several economic and structural barriers that imposes limits on their digital participation, which reinforces wider social injustices.

According to a Pew Research Center finding, the expense of residential broadband services makes Black and Hispanic Americans more likely to rely on cellphones as their main internet source than White Americans (Vogels, Perrin, Rainie, & Anderson, 2021). Because smartphones provide less flexibility than traditional computers for tasks like doing homework, accessing government services, or working remotely, this reliance on mobile-only access frequently restricts the utility and efficacy of digital interaction. Same could be said of surveillance, which is predominantly employed to protect Americans generally, prevent cybercrime, and maintain public order. However, it is said to be used indiscriminately, chiefly against low-income people and members of racial and ethnic minorities, to the point where it breaches their ostensibly protected personal privacy, turning it into public vigilantism (Iannacci, 2019).

The origin of the digital divide can be traced back to historical policies that created unequal access to resources and infrastructure. Differences in internet infrastructure and technology investment among Black and Hispanic groups had its roots from practices like redlining, which hindered the financial services and investment access of certain neighbors (Noble, 2018). These pre-existing divides only became amplified and more apparent in these days of high digital access, beginning from the COVID-19 pandemic, which compelled many elements of daily life to shift online. Without reliable internet and technological devices, marginalized communities faced disruptions to their education, employment, and health services, which only worsened the limitations they already faced (Turner-Lee, 2019).

Digital literacy, which is the skills needful for the efficient use and navigation of the internet resources efficiently, is another issue that is related to the digital divide. Even in an avalanche of access, marginalized groups are most likely digital illiterates, which poses a bigger challenge to fully participate in the digital world. This is because persons who lack internet or technology literacy may lose out on important information, educational opportunities, and jobs since they lack what it takes to close the gap (Eubanks, 2018). Because the prejudices of technology developers and blind spots frequently result in tools that unintentionally hurt or ignore marginalized groups, the lack of inclusive representation in digital and artificial intelligence (AI) technologies exacerbates these problems.

Objectives of the Study

This study aims to explore the significance of inclusivity in AI development and governance, focusing on how fair data privacy regulations and inclusive policies can support equitable access and opportunities for marginalized groups. The study will achieve this by examining the current state of data privacy and artificial intelligence governance in the United States, with an emphasis on how these frameworks affect marginalized communities, identifying risks related to data privacy and AI that disproportionately impact underrepresented groups, analyzing the role of surveillance capitalism and algorithmic bias in widening the digital divide. The work will also evaluate the ethical frameworks and accountability mechanisms within the AI industry, assessing the inclusivity and transparency of these structures in relation to marginalized communities, and highlight how inclusive policies benefit marginalized groups and the U.S. economy. The study will provide recommendations for advancing fair data protection and inclusive AI governance in the United States, in order to assist and benefit both marginalized groups and the general society welfare.

DATA PRIVACY RISKS AND IMPACT OF LACK OF INCLUSIVITY IN AI GOVERNANCE IN THE U.S.

As a general-purpose technology, AI is wide-reaching and rapidly permeating products, sectors, and business models across the globe. From surveillance capitalism and racial bias in facial recognition technology to digital divide in AI human resource and healthcare, the current state of data privacy and artificial intelligence governance in the United States, however, raises concerns and risks that disproportionately impact underrepresented and marginalized groups (OECD, 2024, p.9).

Surveillance Capitalism

Surveillance capitalism, coined by Shoshana Zuboff, refers to the commodification of personal data by tech companies for predictive and control purposes Harvard Law Review (2023). It describes an economic system where personal data is monetized, with companies using AI- driven platforms to collect large quantities of data to shape and predict behavior, often resulting in targeted marketing that reinforces existing social hierarchies. For marginalized communities, this pervasive data collection can lead to heightened surveillance and exploitation, with companies or governments using algorithms that disproportionately affect specific groups (Zuboff, 2019). Algorithm bias further compounds these issues, with AI models embedding societal biases into decision-making processes. In law enforcement, for instance, predictive policing algorithms trained on historical crime data frequently reinforced racial profiling, disproportionately impacting communities of color. AI systems rely on past data, they risk perpetuating existing inequalities rather than offering objective analysis (Pasquale, 2015).

In 2012, the Chicago Police Department began using predictive policing algorithms under the SSL (Strategic Subject List) program, which assigned “threat scores” to individuals based on data such as prior arrests and known associations. This list was used to predict individuals likely to be involved in violent crime, either as a victim or a perpetrator. However, the system faced significant criticism over concerns that it reinforced existing biases, particularly in predominantly Black and lower-income neighborhoods, and questions about its effectiveness eventually led to its suspension in 2020. The New York Police Department (NYPD) and Central Intelligence Agency (CIA) surveilled Muslim neighborhoods, restaurants, mosques, stores, and student groups for over six years after September 11, 2001, listening in on conversations, recording license plates, and taking videos (Bedoya, 2016; Goldman & Apuzzo, 2012). Over a decade after 9/11, a 2017 Pew Research Center survey found that 18% of Muslim American respondents still experienced being “singled out by airport security” (Pew Research Centre, 2017).

The U.S. government's response to public protests over egregious policing patterns has, over the years, raised various concerns over the appropriate use of surveillance, especially when primarily focused on communities of color (Turner-Lee & Chin-Rothmann, April 7, 2022). In 2015, the Baltimore Police Department reportedly used aerial surveillance, location tracking, and facial recognition to identify individuals who publicly protested the death of Freddie Gray (Rector & Knezevich, October 18, 2016; Ovide, June 9, 2020) Similarly, after George Floyd was murdered in 2020, the U.S. Department of Homeland Security (DHS) deployed drones and helicopters to survey the subsequent protests in at least 15 cities (Kanno-Youngs, 2020).

Beyond African Americans, mass government surveillance was evident in the China Initiative program, which the Department of Justice (DOJ) launched in 2018 to prevent espionage and intellectual property theft and formally ceased in February 2022 (U.S. Department of Justice, 2020; Lucas, 2022). Although the China Initiative aimed to address national security threats from the Chinese government, it manufactured wider distrust and racial profiling of Chinese American academics, including those who were U.S. citizens or who lacked ties with the Chinese Communist Party. It led to several false arrests, including those of Temple University professor

Xi Xiaoxing, UCLA graduate student Guan Lei, University of Tennessee professor Anming Hu, and National Weather Service scientist Sherry Chen (German & Liang, 2022; Lee, 2021). Like with other historically-disadvantaged populations, government surveillance of Asian Americans is not a new phenomenon. As an example, the U.S. government monitored the broader Japanese American community for years even prior to World War II, including by accessing private communications and bank accounts, and eventually used census data after 1941 to locate and detain 120,000 people in internment camps (Loureiro, 1994).

Demonstrating similar profiling of an entire community, social media platforms like Facebook have come under fire for algorithmic targeting, which has enabled landlords to exclude out prospective tenants on the ground of race or other demographic factors, thereby felicitating digital redlining (Wallace, 2024).

Racial Bias in Facial Recognition Technology

Facial recognition has become a commonplace tool for U.S. law enforcement officers at both the federal and municipal levels. Out of the approximately 42 federal agencies that employ law enforcement officers, the Government Accountability Office (GAO) discovered in 2021 that about 20, or half, used facial recognition (U.S. Government Accountability Office, 2021). In 2016, Georgetown Law researchers estimated that approximately one out of four state and local law enforcement agencies had access to the technology (Garvie et al., 2016). On the procurement side, Clearview AI is one of the more prominent commercial providers of FRT to law enforcement agencies. Since 2017, it has scraped billions of publicly available images from websites like YouTube and Facebook, and enables customers to upload photos of individuals and automatically match them with other images and sources in the database (Hill, 2020). As of 2021, the private startup had partnered with over 3,100 federal and local law enforcement agencies to identify people outside the scope of government databases. To put this tracking in perspective, the FBI only has about 640 million photos in its databases, compared to Clearview AI's approximately 10 billion (Watkins, 2019).

Facial recognition, which has become one of the most critical and commonly-used technologies, poses special risks of disparate impact for historically marginalized communities. In December 2020, the New York Times reported that Nijeer Parks, Robert Williams, and Michael Oliver - all Black men - were wrongfully arrested due to erroneous matches by facial recognition programs. Recent studies demonstrate that these technical inaccuracies are systemic. MIT and former Microsoft researchers Buolamwini and Gebru (2018) published an analysis of three commercial algorithms developed by Microsoft, Face++, and IBM, finding that images of women with darker skin had misclassification rates of 20.8%-34.7%, compared to error rates of 0.0%-0.8% for men with lighter skin. Buolamwini and Gebru also discovered bias in training datasets: 53.6%, 79.6%, and 86.2% of the images in the Adience, IJB-A, and PBB datasets respectively contained lighter-skinned individuals (Buolamwini & Gebru, 2018). In December 2019, the National Institute of Standards and Technology (NIST) published a study of 189 commercial facial recognition programs, finding that algorithms developed in the United States were significantly more likely to return false positives or negatives for Black, Asian, and Native American individuals compared to white individuals (U.S. National Institute of Standards and Technology, 2019; Singer & Metz, 2019).

Black and other persons of color are more likely to be mistakenly identified for a crime they have no connection to when the consequences of bias in some policing practices combine with the uneven accuracy rates of facial recognition technology.

Gender Bias in AI Hiring Algorithms

Research show that there has long been a worry that algorithms could perpetuate gender inequality through the data they are trained on or the people who create them (Angwin et al., 2016). For instance, searches for names that sound particularly Black are more likely to result in ads for arrest records, job search ads for high-paying jobs are less likely to be shown to women (Harwell, 2019), and image searches for occupations like CEO yield fewer images of women (Kay et al., 2015). Natural language processing algorithms have been shown to encode language in gendered ways, and facial recognition systems, which are being utilised more and more in law enforcement, perform poorly when it comes to identifying the faces of Black and female people (Aratani, 2018).

So, although AI hiring algorithms have gained traction due to their efficiency in evaluating large volumes of applications, studies reveal that these algorithms often reinforce gender inequalities (Akselrod, 2021). This bias results from historical data that shows male dominance in particular industries, which leads AI to give preference to experiences and credentials that are often associated with men.

In 2018, for instance, Amazon scrapped an AI recruiting tool that was found to downgrade résumés with the word "women" or references to women's colleges. This happened as a result of the algorithm being trained on historically hiring data that was predominately male (Knight, 2021). The discrimination of the tool against women in technical positions became a crucial barricade to gender equality in the workplace.

Digital Divide and Healthcare AI

AI's integration into healthcare holds promise for improved diagnosis and personalized treatment, as it also risks reinforcing the digital divide (FTC, 2020**)**. Marginalized communities often lack access to high-quality healthcare and the digital tools that support AI-driven health innovations, limiting their ability to benefit from advancements like predictive diagnostics. When AI models are trained predominantly on data from well-served populations, they are less accurate in predicting health outcomes for minority groups, which exacerbates health disparities (Nelson, 2012).

A study by Obermeyer et al. (2019) found that a widely-used commercial predictive health management algorithm tool in the U.S. reveals racial bias. The algorithm, intended to assess patients' health risks for care program enrollment, assigns similar risk scores to Black and White patients, yet Black patients at high-risk scores show 26.3% more chronic illnesses than their White counterparts. For instance, among patients in the 97th percentile of risk, Black patients averaged 4.8 chronic conditions versus 3.8 for White patients. The study further illustrates this by depicting the racial discrepancy in chronic illness burden via risk score and suggests that Black patients, under the original algorithm, are systematically underrepresented in high-risk care programs due to this misalignment. The algorithm prediction is based on healthcare costs rather than health status and it inadvertently favors White patients due to disparities in healthcare access.

IMPORTANCE OF INCLUSIVITY IN AI GOVERNANCE AND DATA PRIVACY

Importance of Fair Data Privacy Regulations

Fair data privacy regulations are essential in today's digital environment, where personal data is frequently utilized and used in ways that individuals may not come to total grasp or consent to. The goal of data privacy regulations is to protect individuals from intrusive data collection practices and guarantee that data usage aligns with privacy rights and ethical standards. This is especially important for marginalized groups, who are often more vulnerable to privacy violations due to systemic biases within AI-driven systems (Turner-Lee & Chin-Rothmann, 2022).

For instance, unregulated facial recognition surveillance may result in disproportionately monitoring communities of color. According to Turner-Lee & Chin-Rothmann (2022), communities of color are more vulnerable to being mistakenly recognized and improperly surveilled by law enforcement technology in the absence of equitable data privacy regulations. This not only violates privacy but can also result in unwarranted legal actions.

When Inclusive Policies Benefit Marginalized Groups and the Economy

Inclusive AI and data privacy policies not only support marginalized communities but also bring broader economic benefits. When AI governance incorporates inclusivity, it enhances fairness, boosts public trust, and helps create a more level playing field, which can foster economic growth and innovation.

When AI tools are developed inclusively, they can improve healthcare access and outcomes for underserved populations. The work of Obermeyer et al. (2019) demonstrated that predictive healthcare algorithms that consider socioeconomic disparities can better serve patients who would otherwise be overlooked in care management programs. This approach not only benefits marginalized communities by addressing health disparities but also reduces long-term healthcare costs and enhances population health, which benefits the economy.

In the workplace, inclusive AI policies promote a more diverse workforce by ensuring that hiring algorithms are free from gender, racial, and cultural biases. As more organizations adopt these policies, they are able to tap into a broader talent pool and foster diverse perspectives that contribute to creativity and innovation. A report by the McKinsey Global Institute found that organizations with greater gender and racial diversity are more likely to outperform less diverse peers in profitability (Hunt et al., 2018). By integrating inclusivity into AI governance, companies can enhance productivity, support equitable economic participation, and stimulate overall economic growth (Nerenz et al., 2019).

ETHICAL CONSIDERATIONS FOR AI GOVERNANCE IN THE UNITED STATES

Ethical AI frameworks serve as foundational guidelines to ensure that AI systems operate within ethical, fair, and transparent boundaries. These frameworks emphasize values like fairness, accountability, and privacy, and often address potential biases in AI-driven systems that impact marginalized communities. Ethical AI development and stringent regulatory policies are needed to prevent misuse, particularly in law enforcement contexts where biases can have life-altering consequences for marginalized individuals (Bohai, 2022). A widely referenced ethical framework in the U.S. is the AI Principles established by the U.S. Department of Defense (DoD), focusing on responsible, equitable, traceable, and governable AI (DOD, 2020). These principles serve as a model for other industries looking to implement ethical standards in AI, especially when algorithms are used in high-stakes scenarios like law enforcement or healthcare.

Independent researchers (Obermeyer et al. 2019) utilized data provided by a large academic hospital in identifying the racial bias in healthcare algorithm. This would be unattainable without the transparency of that hospital and the researchers' independence.

In response to privacy and ethical concerns, and after the protests over George Floyd's murder in 2020, some technology companies, including Amazon, Microsoft, and IBM, pledged to either temporarily or permanently stop selling facial recognition technologies to law enforcement agencies (Dastin, 2022). But voluntary and highly selective corporate moratoriums seem insufficient to protect privacy, since they do not stop government agencies from procuring facial recognition software from other private companies (Dayo-Ajanaku, 2022). Moreover, a number of prominent companies have noticeably not taken this pledge or continue to either enable or allow scaping of their photos for third-party use in facial recognition databases. Furthermore, government agencies can still access industry-held data with varying degrees of due process, for example, although they would require a warrant with probable cause to compel precise geolocation data from first-party service providers in many cases, they might be able to access a person's movement history without probable cause through other means, including by purchasing it from a data broker (Morrison, 2021).

CONCLUSION AND RECOMMENDATIONS

Summary of Key Findings

This study highlights the critical intersections between AI governance, data privacy, and inclusivity, especially concerning marginalized communities in the U.S. The study finds that the digital divide remains pervasive, affecting access to digital literacy, resources, and the benefits of AI advancements. AI-driven technologies, including predictive policing, hiring algorithms, and facial recognition, exhibit systemic biases.

The study further finds that the technological and privacy prejudices disproportionately impact people of color and economically disadvantaged individuals, exacerbating inequities. Surveillance capitalism and data commodification are deeply entangled with racial and economic biases, as shown through practices like predictive policing and algorithmic assessments in healthcare, emphasizing the need for an inclusive approach to AI governance to prevent widening the marginalization gap further.

It must be stated that the research found that gender bias in AI hiring tools, as seen in Amazon's now-discontinued recruiting algorithm, highlights the broader issue of lack of inclusivity in tech while reflecting the existing gender disparity in tech fields. The study further finds that the lack of inclusivity in tech and AI governance has substantial implications, for marginalized groups who often face discrimination and inequitable outcomes in AI-driven systems. Beyond the implication for marginalized groups, it affects the performance and productivity of companies, which in turn affects the United States economy.

Recommendations for Fair Data Protection and Inclusive AI Governance in the U.S.

To address the issue of data privacy and AI algorithm bias for marginalized groups, the United States government must implement rigorous data privacy laws as strengthening data privacy laws similar to the EU's GDPR would help protect individual rights, especially for vulnerable groups disproportionately affected by data misuse. In this light, the study recommends mandatory transparency for companies on data collection, consent practices, and data-sharing policies.

To mitigate privacy breach of colored people and prevent AI algorithm bias, the U.S. government should adopt enforceable guidelines for ethical AI similar to the Department of Defense's AI Principles, focusing on transparency, fairness, and equity. Incorporating ethical considerations across AI development, from training data selection to deployment, is essential for reducing biases as voluntary and highly selective corporate moratoriums like those of Amazon, Microsoft, and IBM in response to the protest of George Floyd's murder are insufficient.

To improve oversight and equity in AI-powered surveillance, the U.S. government should adopt several measures. First, extend equity assessments to evaluate facial recognition and geolocation data access, considering privacy and civil rights implications. Congress should enact proposed laws, such as the George Floyd Justice in Policing Act and the Facial Recognition and Biometric Technology Moratorium Act, to restrict federal agencies' use of facial recognition and require warrants for long-term surveillance. Although these would not apply universally, federal guidance could encourage state and local governments to specify appropriate contexts and processes for using surveillance technologies. Also, the government should establish training for law enforcement on racial bias, implicit bias, and mental health, while encouraging community participation in oversight boards.

While the Federal Trade Commission (FTC) is has partly addressed data privacy issues and AI- driven algorithmic bias in companies through various regulations and enforcement strategies, particularly under the authority granted by Section 5 of the FTC Act, the Fair Credit Reporting Act (FCRA), and the Equal Credit Opportunity Act (ECOA), the approach can be further strengthened by creating a dedicated set of AI transparency and accountability standards, specifically aimed at algorithms affecting sensitive areas like credit, hiring, and biometric surveillance. These standards would require companies to document how AI models are developed, tested, and deployed, including transparency on training data sources, model updates, and testing methodologies to detect and mitigate bias. Clear guidance would also help businesses understand expectations, potentially reducing unintentional bias risks and improving compliance across industries. In addition, expanding the FTC's capacity to perform regular AI audits by requiring companies to submit periodic impact assessments, especially for high-impact sectors like finance and healthcare, would enable more consistent oversight. These audits could assess whether algorithms continue to meet fairness standards over time, as models might evolve or perform differently in practice.

Lastly, companies are advised to support inclusive AI development by diversifying data sets and ensuring demographic representation in training data for AI models, especially in sensitive applications like healthcare and law enforcement. Integrating diverse viewpoints within AI development teams helps identify potential biases early in the process.

Areas for Further Research

Research into community-driven privacy policies could highlight effective models for balancing public safety with individual privacy rights. Such studies, which would offer practical frameworks for inclusive data privacy protections and surveillance measures, is recommended.

Further research is needed to advance technical solutions for mitigating biases in algorithms. This includes exploring ways to create fair, representative datasets and developing new methods for detecting and reducing biases in AI systems.

The effects of biased AI systems on employment, healthcare, and justice outcomes require deeper investigation. Understanding the lasting impact of these biases on marginalized communities' social mobility and economic participation could guide more equitable AI policies. Future research is recommended in this area.

Conclusion

Addressing the digital divide requires a dual approach that goes beyond merely expanding access. It calls for creating inclusive and equitable digital environments that enable marginalized communities to fully participate in the opportunities of the digital age. As technology becomes integral to governance, healthcare, and education, it is crucial to ensure that all individuals have access to the necessary tools, skills, and digital literacy to engage effectively in these areas. Digital inclusion is essential to prevent marginalized groups from being left further behind and to foster an equitable society.

The development of generative AI, fueled by vast global datasets, underscores the need for coordinated global efforts in privacy standards. With actors involved in AI's lifecycle spread across jurisdictions, synchronized guidelines are essential to address privacy challenges effectively. Ethical AI frameworks, alongside bias-mitigation techniques, are critical to developing systems that promote justice and inclusivity, reducing the risks of surveillance and exploitation of vulnerable groups.

Comprehensive data privacy regulations, like the EU's GDPR, set an example by enforcing strict data usage requirements and enhancing individual control over personal information. Such frameworks are vital for ensuring that the benefits of AI and digital advancements are distributed fairly, providing marginalized groups with equal protection and opportunities in a rapidly digitalizing world. Through thoughtful governance, rigorous oversight, and continued research into bias mitigation, the U.S. can set a precedent for responsible, inclusive AI that fosters a fairer society for all.

REFERENCES

[1] ALU. (2006, April 20). Statement - The Japanese American citizens league. *American Civil Liberties Union*. https://www.aclu.org/other/statement-japanese-american-citizens-league

[2] Anderson, M., & Perrin, A. (2018). *Nearly one-in-five teens can't always finish their homework because of the digital divide*. Pew Research Center. Retrieved from http://www.pewresearch.org/staff/andrew-perrin

[3] Akselrod**,** O. (2021, July 13). How artificial intelligence can deepen racial and economic inequities. *ACLU https://www.aclu.org/news/privacy-technology/how-artificial-intelligence-can- deepen-racial-and-economic-inequities*

[4] Angwin**,** J., Larson**,** J., Mattu**,** S., & Kirchner**,** L. (2016, May 23). Machine bias.*ProPublica* www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[5] Aratani**,** L. (2018, April 3) Secret use of census info helped send Japanese Americans to internment camps in WWII. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/retropolis/wp/2018/04/03/secret-use-of-census- info-helped-send-japanese-americans-to-internment-camps-in-wwii/

[6] Bedoya, A. M. (2016, January 18). What the FBI's Surveillance of Martin Luther King Tells Us About the Modern Spy Era. *Slate Magazine*. https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says- about-modern-spying.html

[7] Bohai. (2022, February 2). Ethical concerns of combating crimes with AI surveillance and facial recognition technology. *Medium*. https://towardsdatascience.com/ethical-concerns-of- combating-crimes-with-artificial-intelligence-surveillance-and-facial-a5eb7a09abb1

[8] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of the Conference on Fairness, Accountability, and Transparency* (pp. 77–91). PMLR.

[9] Civil Liberties Union for Europe. (2021, October 5). *What is marginalization? What to do if you are marginalized?* Retrieved from https://www.liberties.eu/en/stories/marginalization- and-being-marginalized/43767

[10] Dastin**,** J., (2022, May 18). Amazon extends moratorium on police use of facial recognition software. *Reuters*. Retrieved from https://www.reuters.com/technology/exclusive- amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/.

[11] Dayo-Ajanaku, J.D. (2022, January 26). How Artificial Intelligence Impacts Marginalized Communities. *Kerkeley Law*. https://sites.law.berkeley.edu/thenetwork/2022/01/26/how-artificial-intelligence-impacts-marginalized-communities/

[12] Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

[13] Fairlie, R. W. (2020). The impact of COVID-19 on small business owners: The first three months after social-distancing restrictions. *Journal of Economics & Management Strategy*, 29(4), 727–740. https://doi.org/10.1111/jems.12400

[14] FTC. (2020). Using artificial intelligence and algorithms. Retrieved from https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-algorithms

[15] Garvie**,** C., Bedoya**,** A., & Frankle**,** J. (2016, October 18). The perpetual line-up: unregulated police face

recognition in America. *Georgetown Law, Center on Privacy & Technology*. https://www.perpetuallineup.org/

[16] German, M., & Liang, A. (2022, January 3). *Why Ending the Justice Department's "China Initiative" is Vital to U.S. Security*. Just Security. https://www.justsecurity.org/79698/why-ending-the-justice-departments-china-initiative-is-vital- to-u-s-security/

[17] Goldman, A., & Apuzzo, M. (2012, August 21). NYPD Muslim spying led to no leads, terror cases. *The Associated Press*. https://www.ap.org/ap-in-the-news/2012/nypd-muslim- spying-led-to-no-leads-terror-cases

[18] Harvard Law Review (2023, March 24). *Cooperation or resistance?: The role of tech companies in government surveillance. Harvard Law Review* 131 (6), 1715 - 1722. Retrieved from https://harvardlawreview.org/print/vol-131/cooperation-or-resistance-the-role-of-tech- companies-in-government-surveillance/

[19] Harwell, D. (2019, December 19). Federal study confirms racial bias of many facial- recognition systems, casts doubt on their expanding use. *The Washington Post*. https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial- bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[20] Hill, K. (2020, January 18). The secretive company that might end privacy as we know it.*The New York Times*. Retrieved from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[21] Hunt, V., Prince, S., Dixon-Fyle, S., & Yee, L. (2018). Delivering through diversity.*McKinsey & Company*. Retrieved from https://www.mckinsey.com/business- functions/organization/our-insights/delivering-through-diversity

[22] Iannacci, N. (2019) June 17). Recalling the Supreme Court's historic statement on contraception and privacy. National Constitution Center. Retrieved from https://constitutioncenter.org/blog/contraception-marriage-and-the-right-to-privacy

[23] Kanno-Youngs, Z. (2020, June 19). U.S. watched George Floyd protests in 15 cities using aerial surveillance. *The New York Times*. Retrieved from https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html

[24] Kay, M., Matuszek, C., & Munson, S. A. (2015). Unequal representation and gender stereotypes in image search results for occupations. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. https://doi.org/10.1145/2702123.2702520

[25] Knight, W. (2021, October 4). Clearview AI has new tools to identify you in photos.*Wired*. https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/

[26] Lee, D. (2021, September 18). Why Trump's anti-spy "China Initiative" is unraveling - Los Angeles Times. *Los Angeles Times*. https://www.latimes.com/politics/story/2021-09- 16/why-trump-china-initiative-unraveling

[27] Loureiro, A. (1994) Japanese espionage and American countermeasures in pre—pearl harbor California. *The Journal of American-East Asian Relations* 3(3), 197–210 Retrieved from https://www.jstor.org/stable/23612532

[28] Lucas, R. (2022, February 24). The Justice Department is ending its controversial China initiative. *NPR*. https://www.npr.org/2022/02/23/1082593735/justice-department-china-initiative.

[29] Morrison, S. (2021, July 31). Here's how police can get your data - even if you aren't suspected of a crime. *Vox*. https://www.vox.com/recode/22565926/police-law-enforcement-data- warrant. National Institute of Standards and Technology. (2019, December 19). NIST study evaluates effects of race, age, sex on face recognition software. Retrieved

[30] from https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex- face-recognition-software

[31] Nelson, L. (2012). *Lessons from Medicare's demonstration projects on disease management and care coordination* (Report No. 2012–01). Congressional Budget Office. https://www.cbo.gov/sites/default/files/112th-congress-2011-2012/workingpaper/WP2012-01_Nelson_Medicare_DMCC_Demonstrations_1.pdf

[32] Nerenz, T., Jameson, P., Walker, R., & Jarreau, B. (2019). Lunch Bucket D&I: Turning Diversity and Inclusion into Competitive Advantage at UMUC Europe. *Journal of Human Resource and Sustainability Studies*, *07*(02), 261–276. https://doi.org/10.4236/jhrss.2019.72016

[33] Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism.*

[34] NYU Press.

[35] Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447–453. https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020- ziad_obermeyer.pdf

[36] OECD. (2024). AI, data governance & privacy: Synergies and areas of international co- operation. *OECD Artificial Intelligence Papers*, (22), 1- 55. https://www.oecd- ilibrary.org/science-and-technology/ai-data-governance-and-privacy_2476b1a4-en

[37] OECD. (2024). AI, data governance and privacy: Synergies and areas of international cooperation. In *OECD Artificial Intelligence Papers*, 1- 55. https://doi.org/10.1787/2476b1a4-en

[38] Ovide, S. (2020, June 9). A case for banning facial recognition. *The New York Times*.

[39] Retrieved from https://www.nytimes.com/2020/06/09/technology/facial-recognition- software.html

[40] Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

[41] Pew Research Center. (2024b, September 23). *U.S. Muslims Concerned About Their Place in Society, but Continue to Believe in the American Dream*. https://www.pewforum.org/2017/07/26/findings-from-pew-research-centers-2017-survey-of-us- muslims/

[42] Rector, K., & Knezevich, A. (2016, October 18). Maryland's use of facial recognition software questioned by

researchers, civil liberties advocates. *The Baltimore Sun*. Retreived from https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html

[43] Singer**,** N. and Metz**,** C. (2019, December 19). Many facial-recognition systems are biased, says U.S. study. *The New York Times*. https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

[44] Turner-Lee, N. (2019). *The digital invisible: How the internet is creating an underclass.*

[45] Brookings Institution Press. Retrieved from https://www.brookings.edu

[46] Turner-Lee, N., & Chin-Rothmann, C. (2022, April 7). Police surveillance and facial recognition: Why data privacy is imperative for communities of color. *Brookings.* Retrieved from https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data- privacy-is-an-imperative-for-communities-of-color/

[47] U.S. Department of Justice. (2020, July 31). U.S. department of justice. information about the department of justice’s China initiative and a compilation of China-related prosecutions since 2018. Retrieved from https://www.justice.gov/archives/nsd/information- about-department-justice-s-china-initiative-and-compilation-china-related

[48] U.S. Government Accountability Office. (2021, July 13). Federal law enforcement agencies should have better awareness of systems used by employees. US GAO. Retrieved from https://www.gao.gov/products/gao-21-105309

[49] U.S. Government Accountability Office. (2021, June 29). *Artificial intelligence: Status of implementing the national security commission’s recommendations.* US GAO. Retrieved from https://www.gao.gov/products/gao-21-518

[50] Vogels, E. A., Perrin, A., Rainie, L., & Anderson, M. (2021). Digital divide persists even as Americans with lower incomes make gains in tech adoption. *Pew Research Center*. Retrieved from https://www.pewresearch.org

[51] Wallace, N. (2023, December 8). *Of spies and G-men: how the U.S. government turned Japanese Americans into enemies of the state*. Densho: Japanese American Incarceration and Japanese Internment. https://densho.org/catalyst/of-spies-and-gmen/

[52] Watkins**,** E. (2019, June 4). Watchdog says FBI has access to more than 641 million ‘face photos.’ *CNN*. https://www.cnn.com/2019/06/04/politics/gao-fbi-face-photos/index.html

[53] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs. http://dx.doi.org/10.1007/s00146-020- 01100-0