10-19-2020

Privacy And The Digital Divide: Investigating Strategies For Digital Safety By People Of Color

Denavious Hoover
Illinois State University, denavious@gmail.com

PRIVACY AND THE DIGITAL DIVIDE: INVESTIGATING STRATEGIES FOR DIGITAL SAFETY BY PEOPLE OF COLOR

DENAVIOUS HOOVER

95 pages

People of color are becoming increasingly concerned with digital privacy. They are concerned about the obfuscated data collection and sharing practices of major social media platforms and the strong entitlement of other users in the online space to their content. This study examines how people of color conceptualize and behave to produce safety in the online space, or, in other words, digital privacy. This study challenges notions that people are not purposeful about privacy in the online space and highlights the voices of people of color, whom are not often included in theorizing or decision making about the online space.

This qualitative study reveals generational differences in the digital privacy strategies of people of color. Participants who are Millennials and Generation X are influenced by intergenerational knowledge when they conceptualize and seek to create privacy. Participants who are from Generation Z lack this knowledge, and, therefore, approach privacy differently. This difference is revealed in the choice of participants that are Millennials and Generation X to self-deplatform from major social media. Instead, Younger participants, who belong to Generation Z, practice strict curation of their online selves. The aim of this strategy is to endure. They believe that future economic and social benefits wait on the other side of disprivacy.

KEYWORDS: race, digital divide, digital privacy, digital participation, digital inequality, internet history

PRIVACY AND THE DIGITAL DIVIDE: INVESTIGATING STRATEGIES FOR DIGITAL SAFETY BY PEOPLE OF COLOR

DENAVIOUS HOOVER

A Thesis Submitted in Partial
Fulfillment of the Requirements
for the Degree of

MASTER OF SCIENCE

Department of Sociology and Anthropology

ILLINOIS STATE UNIVERSITY

2020

PRIVACY AND THE DIGITAL DIVIDE: INVESTIGATING STRATEGIES FOR DIGITAL SAFETY BY PEOPLE OF COLOR

DENAVIOUS HOOVER

COMMITTEE MEMBERS:

Livia K. Stone, Chair

Aaron Z. Pitluck

James Stanlaw

ACKNOWLEDGMENTS

Firstly, I would like to thank my thesis chair Dr. Livia Stone who supported and encouraged me to find my own voice. Dr. Stone dedicated many invaluable hours of intensive listening and purposeful challenging, even when I called unexpectedly or emailed late in the night. I am forever thankful for Dr. Stone’s kind yet unyielding belief in my research. I would also like to thank Dr. Aaron Pitluck and Dr. James Stanlaw for a similar spirit in supporting me through my academic career and research. Without the thoughtful comments and constructive challenges from my thesis committee, this research and thesis would not have been possible. I am deeply grateful for your support, and I sincerely thank you. Second, I would like to thank my dear friends and mentors Heather Jagman and Arek Dreyer. They inspire me everyday, and I would not have embarked on this academic journey without their encouragement. Third, I would like to thank many of my dear friends who entertained my longwinded tangents on theories of digital privacy and inequality even when we were in completely non-academic situations. Lastly, and most importantly, I would like to thank my family, especially my parents, Ulrika Bryant, Elmore Bryant, and Jerald Massie. They have been patient and understanding despite the long hours of interviewing, analysis, and writing which cut into our time together. They have supported me tirelessly and have never wavered in their support of my decisions to pursue my academic inclinations. Ultimately, I would like to thank all who were involved during these difficult times of Covid-19 who helped make my thesis possible. Additionally, I would like to thank Dr. Nobuko Adachi and Professor Sanae Ferrier, without whom I would not be in academia today. Thank you.

D. H.

CONTENTS

CHAPTER I: INTRODUCTION

“Please stop killing us, that’s it!” — “The people on YouTube are not killing you, so…” This was the beginning of a contentious exchange between a white male YouTube and Twitch Streamer for the Zach and Matt Show and a Black woman-of-color protestor. It was live-streamed from the George Floyd and Breonna Taylor protests in Washington D.C.

Just moments before the argument began, the two had been watching a small group of protestors expressing their outrage on a window with “Fuck 12” written on it. As the streamer pans the camera around, a hand goes up to block the lens. Then an off-camera speaker asks, “Is this for a news organization?”. The streamer replies obliviously, “So you’re currently on YouTube, and there’s twenty-eight thousand people watching”—The camera starts to point at the off-camera person, and the off-camera person continues to use their hands to block the camera. It’s appears to be a woman of color. She is wearing a mask, but uses both hands to shield her face from the camera— “So if you want to shout out your instagram, have at it!” She responds emphatically, “I don’t!” After a few moments, and as the camera follows her she says, “Please stop killing us, that’s it!”, and the streamer quickly responds in contestation, “The people on YouTube aren’t killing you, so…” She retorts with, “So it’s ok to watch us when we are like protesting and stuff, but you don’t want to stand with us.” The streamer’s white fragility begins to show as he says “she is going to make him upset”. He tries to legitimize himself and his frustration at her words by explaining that earlier in the day he had been shot by rubber bullets. The woman of color dismisses him, and then he calls her a bitch. As the crowd comes to her defense, he continues to record. A tussle ensues, and viewers can hear her say that “he’s not here to protest”. Another person of color emerges from the crowd to rescue the streamer, and the woman of color he had been arguing with says, “If you are on our side, then shut up and give us the mic!” His response is a veiled threat. “Twenty-eight thousand people seeing you behave like an idiot!” She responds, “and twenty-eight thousand people seeing you behave like a racist dumbass!” Earlier that week, The Zach and Matt Show was criticized because the same host explained to viewers on Twitch that he was attending the protests to film violence.

This vignette shows the precariousness of the online space for people of color. The streamer repeatedly tried to film the woman’s face despite her dismay at being filmed. In addition, the streamer’s intentions for attending the protests are made clear by his suggestion that she “shout out” her instagram handle to his twenty-eight thousand viewers. He is clout chasing instead of protesting, and, in the process of doing so, he is exploiting the struggle of people of color and putting them directly in danger. He cannot understand or refuses to acknowledge that by broadcasting people of color’s faces during the protests he puts them at a higher risk of suffering their oppressors’ ire. And when the very people of color he seeks to exploit make him confront his white privilege, he lashes out. He makes it clear that his twenty-eight thousand followers are a weapon that may be exacted upon the woman of color who confronts him.

Similar behaviors are practiced at all levels and corners of society. Even the forty-fifth President of the United States participated in this type of weaponization of digital content. On Friday, June 26th, 2020, former President Donald Trump tweeted “wanted posters” for protester. Those featured in the tweets were alleged to have removed a statue near the Whitehouse. By posting those photos, the former President engaged in the same weaponization of his followers as the streamer for the Zack and Matt Show. He knew that his millions of followers could not assist him to locate the individuals in his posts. His tweet was a threat to those who allegedly toppled the statue and those who are considering any tangible form of resistance: All eyes are on you! Those who took the photos are equally as complicit; in their eagerness to exploit the struggle of people of color, they deliver Black people into the hands of their oppressors.

The constants in this cycle of online *disprivacy*, a term that I believe more accurately describes the condition and commodity that results from these situations, are the white voyeur and the bodies of people of color. When an institution or person exposes and exploits a person of color, such as in the case of trauma porn (Kanengo 2020), they are creating a commodity. The aim is not to invade privacy to gain some thing. The thing that is sought, traded, and sold is the disprivacy itself. We need to understand how people of color exist in the online space, which violates, exploits, and then disregards them. We need to understand how people of color negotiate participation and privacy strategies in the online space. How do they find or create safety? How do they react when they become the targets of violence in the digital space? Do they seek allyship? This research seeks to investigate these questions.

CHAPTER II: REVIEW OF LITERATURE

The Inception and Initial Conception of the Online Space (1969 - 1989)

The first iteration of the internet was developed at the Advanced Research Projects Agency (ARPA), and so it is named the ARPA network (ARPANET). The impetus for the creation of ARPA and ARPANET directs us to a guiding prominence of governmental aims. ARPA was created as a sub-agency of the Department of Defense (DoD) in 1958. The agency was a direct response to the increasing distrust between the U.S. and the U.S.S.R. during the mid Cold War period. In response to the launch of the soviet space probe Sputnik I, the DoD created ARPA with the expressed mission to develop cutting edge technology that would baffle adversaries (Lukasik 2011, 6). Once NASA was established in 1959 to support U.S. aims for space in a non-defense manner, ARPA focused on terrestrial technologies. In 1961 DoD named former MIT professor Jack Ruina to head ARPA, and the ARPA mission was updated in 1962 to "support research on the conceptual aspect of command and control and to provide a better understanding of organizational, informational, and man-machine relationships" (7). To support the new mission, Ruina hired many new but respected staff from academia and government. These new members, which included J.C.R. Licklider, Robert Taylor, Larry Roberts, and Paul Baran, conceptualized what would come to be known as a "network" to eliminate redundancy and mend dysfunction between ARPA teams and those who relied upon their information and research. Thus, the work on ARPANET began.

The 1963 Limited Test Ban Treaty (LTBT) also encouraged real world application of ARPA's networking research. Officially known as the *Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and Under Water*, the 1963 LTBT notably does not outright prohibit tests of nuclear weapons underground. The treaty stipulates that underground tests are only banned if they will pollute neighboring nations with radioactive materials (Article I). Unfortunately, there was no reliable way to discern underground tests from tremors at the time, and the U.S. Nuclear Test Detection Office was interested in using ARPA to figure out a means of reliable detection in order to negotiate a total ban. ARPA decided seismic arrays (sensor systems which could differentiate between earthquakes and underground testing) would be the best solution. In 1969, while ARPA worked on the Vela program's seismic arrays, the ARPANET came online with four connected computers within the U.S. The use of ARPANET to network with the Norwegian Seismic Array (NORSAR) and the National Physics Laboratory in London quickly followed (Njølstad 2007, 666; Bing 2009, 28). Both network connections were complete by 1972, and the first signs of an internet, a truly online space, emerge.

ARPANET was not publicly announced until 1972 at the first International Conference on Computer Communications (ICCC), but many other networks were already underway. However, the public, having become increasingly concerned about privacy on the nascent internet, demanded answers. The root of the publics' concern about U.S. computer networks stemmed from the National Data Center controversy of the 1960s. In 1965, the U.S. government announced that it would centralize multiple databases which were formed of data gathered from the public since the advent of computers. Once the public understood the extent to which the government collected individuals' information — billions of data points, public outrage soon followed (S. Rep. No. 62-032 1971). People were worried about being targeted for their political activism, religious beliefs, and even for their household spending habits. Specifically of political activism, and with the FBI's response to the civil rights movement on his mind, author Arthur R.

Miller remarked in the 1971 senate judiciary constitutional rights subcommittee hearing on Federal Data Banks, Computers and the Bill of Rights that:

> The development of dossiers on people pursuing lawful social and political activity simply bears little relationship to the function of the military, even during periods of social unrest, especially when many of the people being scrutinized are extremely unlikely to engage in any unlawful activity, and when the selection of surveillance suspects seems to be motivated by what must simply be called an incredibly simplistic view of who are the good guys and who are the bad guys, who wears a white hat and who wears a black hat. (S. Rep. No. 62-032, 10)

The heated debates of the mid 60s and early 70s resulted in only two substantive legislative changes: the "Omnibus Crime Control and Safe Streets Act of 1968", which limits wiretap for policing, and the "Fair Credit Reporting Act of 1971", which assigned the right to notice of negative impacts to credit standing to the public (S. Rep. No. 35-024, 1974, 4). The issue of privacy became more complicate when the FBI's National Crime Information Center (NCIC), which maintained and networked information for law enforcement, gave out "erroneous data" repeatedly which resulted in brutality, arrest, and warrants for innocent people (Licklider and Vezza 1978; Hand 1982).

In the 1975 senate judiciary committee's science, technology, and commerce subcommittee hearings on surveillance technology, ARPA and computer experts could not agree on the security of domestic data from ARPANET: "The public version of the research network is the APRAnet, a system linking Universities, military bases, and think tanks. The CIA, NSA, and DIA also use the ARPAnet, but ARPA officials insist it is not used for surveillance purposes. Computer experts, however, say that anyone with a terminal, a telephone, and the proper identification passwords, can access the ARPAnet. Several experts said that the ARPAnet could be expanded by the telephone, to include other Government agencies." (Surveillance Technology 1975, 13).

In essence, any government agency could utilize ARPAnet by simply recruiting a credentialed person. This did not help ease the public's concerns over privacy expressed in the prior hearings. The message was loud and clear: the public was being watched; computers were facilitating the storage of massive amounts of citizen data; and networks would allow for expansive access (H. Doc. No. 63-552, 1976; Krauss 2011).

In 1979, the University of Wisconsin made a proposal to the National Science Foundation (NSF) to develop its own network. ARPA researchers and staff had been emailing, file sharing, and logging in remotely for years by that time, and other researchers wanted parity. The network would provide non-DoD associated researchers with a means of swift, reliable communication, information sharing, and hardware access. This initial proposal for the Computer Science Research Network (CSNET) was rejected. Of the three major considerations provided, the most surprising was the "belief that the CSNET project was proposing to reinvent ARPANET technology; this perception was reinforced by the lack of any gateway between the ARPANET and the proposed CSNET" (Denning, Hearn, and Kern 1981, 4). In the review process for the proposal, CSNET was directed to use ARPA technologies. The project was approved on this and one additional condition: that NSF appoint a project manager for CSNET to direct the network for its first two years of operation. While the result of this behavior by NSF is generally seen as a positive, the ARPA backed TCP/IP protocols (these protocols govern how computers "talk" to each other) are still in use today, NSF's demands killed an opportunity to conceptualize the internet without government interference. Requiring the use of TCP/IP and a connection to ARPANET assured the government control and access to all research done on CSNET (free access by ARPA researchers was also a requirement), but it eliminated an opportunity for reflexivity. In other words, the ideas of CSNET were stifled under the NSF's necessity for structures akin to governmental hierarchy (Rogers 1998, 215-216). The effects of this decision are immeasurable because this allowed ARPANET to define the technologies, protocols, policies, and norms of the wider internet. We still employ many of those ARPANET standards today. The Computer Science Network (CSNET) came online in 1981 to much excitement within the scientific community. The passing of the baton from ARPA to the NSF seemingly marked a significant break from the mentality that created the early internet, and in 1989, five years after the establishment of the Nation Science Foundation Network (NSFNET), ARPANET was shut down.

The first iteration of the internet was the ARPANET; it was conceptualized and created without the input or knowledge of the public. The network was created to fulfill the premiere security needs of the government during the Cold War. As the internet grew and diversified, the ARPANET remained the backbone of the online space. Scientific, commercial, and military all coexisted in the same online space, and thus the rules of the primary owner became the norms of the latter. During the rise of the online space there are three recognizable trends that emerge: the guiding prominence of governmental aims, public pessimism about online privacy, and technology gatekeeping. Robert Kahn, the inventor of the networking protocols on which the modern internet rely, predicted before the first International Computer Communications Conference (ICCC) that "the social implications of this field are a matter of widespread interest that reaches society in almost all walks of life; education, medicine, research, business and government"

(Kahn 1972; RFC371). For the first decades of the internet, and an online space, the potential for these changes, foreseen by Kahn, was stifled.

The internet existed, and arguably still exists, in two forms: the network of the state and the network of the people. Since the inception of the online space, these two forms intermingle, support, and compete with each other. Presently, the use of the online space as entertainment, education, and expression is dominant; many perceive the internet as liberating. Conversely, the dawn of the internet, and the online space, supported U.S. security aims and was seen as an exclusive space. The initial digital divide was purely access because the government wholly controlled the technology, infrastructure, research, and people who could access the internet.

Urban Minorities and Digital Privacy (1967-2001)

Urban areas are defined by the U.S. Census Bureau as “Urbanized Areas (UAs) of 50,000 people or more” and “Urban Clusters (UCs) of at least 2,500 and less than 50,000 people” (US Census Bureau 2020). In everyday speech, urban conjures images of high-density commercial high rises. However, for some it summons images of impoverished Black communities. For the purposes of this research, minority is broadly defined as a certain minority status and otherness which includes racial, sexual, political, and religious minorities. This allows for an investigation that is critical, intersectional, and discursively open. While not explicitly referenced as urban minorities, these peoples who are othered by the majority have been forced to negotiate privacy in the online space from nearly the inception of the online space. ARPANET and the various networks it spawned were direct products of the espionage aims of a Cold War mentality. This mentality necessitated surveillance and action internally as much as it did externally. While the DoD surveilled Russians using the ARPANET, the FBI monitored people in the homeland.

The precedence of monitoring urban minorities using computer technologies began with the Counter Intelligence Program (COINTELPRO) in 1959. The program was established at the snap of the Cold War as an anti-communist effort. However, the targets of the programs new surveillance methods and technologies were familiar social others. J. Edgar Hoover specifically crafted COINTELPRO operations to spy on Black and Indigenous rights groups, women's rights groups, immigrant rights groups, and LGBT rights groups (Johnson 2006). The methods of the program were highly controversial but unknown to the public. Surveillance was the least of the operations. FBI agents operating under COINTERLPRO directives intimidated, coerced, and tortured members of the Black Panther Party and other groups (Taylor 2019). These were methods that were developed in cohort with the CIA in their efforts to undermine Vietcong resistance (Packard 2020). Although many in government became weary of the program in its later years, most saw the program as a huge success. J. Edgar Hoover was granted extreme autonomy by legislators and was unabashed in his extensive use of power (Hoerl and Ortiz 2015; Steve 2018).

COINTELPRO operations were formally ceased in 1971, one year before Hoover's death, because of investigations into the killings of Fred Hampton and Mark Clark. Fred Hampton was a young activist that who through his work in the National Association for the Advancement of Colored People (NAACP) and Chicago chapter of the Black Panther Party (BPP) excited the Black (Power) Liberation Movement in Illinois. After he became the State Chairman of the Illinois BPP, the FBI identified him as an unacceptable aberrant and devised a method to manipulate and assassinate him (Churchill and Wall 1990). Mark Clark was also a rising star targeted by the FBI and Hoover explicitly. He was also assassinated on December 4, 1969 while on security duty that night at the Hampton residence. Information on many organizations including the BPP were some of the first to be kept in national databases and utilized to carry out missions. This included the floor plans of Hampton's home which had been charted by a FBI mole who had infiltrated the BPP. The following is an account of that night from the African American Heritage government archives website:

> On the evening of December 3, 1969, William O'Neal, who was employed by the FBI to infiltrate the BPP, slipped a powerful sleeping drug into Hampton's drink then left. Officers were dispatched to raid his apartment. They stormed in and opened fire, killing his security guard. Then they opened fire on Hampton's bedroom where he laid unconscious from the drug with his sleeping, almost nine-month-pregnant fiancee. After the gunfire, he was found to only be wounded and not dead. Upon that discovery, an officer shot him twice in his head and killed him. The remaining seven Panthers who were not killed were all arrested and indicted by a grand jury on charges of attempted murder, armed violence, and a variety of weapons charges. These charges were eventually dropped when during a later investigation, it was discovered that Chicago Police fired ninety-nine shots while the Panthers only shot once. (USNARA 2020, para. 2)

This is one of many examples of the blatant illegal actions by the FBI as part of COINTELPRO operations. It is also simply one example of how new data management and dissemination techniques allowed the FBI to coordinate domestic attacks against urban minorities on U.S. soil. The ensuing investigations led to the end of COINTELPRO in disgrace. Pyle (1974 cited in Packard 2020) identifies the FBI COINTELPRO operations as drivers of networking technologies because the FBI wanted a service that would allow for expedient retrieval of whole records, but also in a ordered format that allowed easier information analysis.

The Nation Crime Information Center was the answer to their calls, literally. Established in 1967, two years before ARPANET, under the Criminal Justice Information Services (CJIS)

Division, NCIC is another infamous creation of Hoover's mind. Once the ARPANET was operational, a police officer could call into an NCIC access point to confirm "hits" on suspected criminals. The central database was established to keep a record of criminals, criminal histories, missing persons, theft, and anything else that was deemed pertinent by the agency. Notably, there was no centralized oversight of the information contributed to the NCIC databases. Participation in the system was voluntary, and the agencies were responsible for "the accuracy, timeliness, and completeness of the record" (Hand 1982, 508).

The inaccuracy of records became a huge issue by the 1980s. NCIC records were notoriously unreliable, but also suspiciously and conveniently inaccurate. It was not out of the ordinary to have a person arrested on a "hit" that was not valid, either because it had been cleared or because it never existed in the first place. Most often these occurred on people who were driving in vehicles or out on the streets. The police would run license plates or other information they received from the person through the NCIC and receive confirmation. Arrest would ensue, but eventually some cases went to court to argue that people's fourth amendment rights were being violated. One such case was that of Harold Decuir in People v. Decuir in Decatur, Illinois. Drug charges against Decuir were dropped on the interpretation that his fourth amendment rights were violated because he was stopped because of a two-month outdated NCIC hit (502). If the information was erroneous, then the search was illegal. This was the argument. Hand (1982) takes a selection of cases to demonstrate the various failures of the NCIC and recommends changes to policy and protocol. Hand and other studies like it (Hemphill 1974) do not cite race or minority status because that is usually not listed in lawsuit proceedings. However, combined with the actions of COINTELPRO, the NCIC arguably disproportionately affected Black people, women, and immigrants during the 1970s and 1980s.

When it became apparent that the fourth amendment would not be sufficient to protect people with the rapid advances of computer and networking technology, digital privacy as an independent concept came to the forefront. Philip Zimmerman, a renowned computer scientist known for his development of cryptographic technologies, argued for the rights of individuals in the online space by arguing that: “It’s personal. It’s private. And it’s no one’s business but yours.” (original 1991, updated 1999). This sounds more like a chant at a protest or a rally cry for battle, and for many it was. Zimmerman was no stranger to activism, and he understood that there would only be one way to attain digital privacy: the people needed to take it. Zimmerman and others saw the unsuccessful attempts to convince legislators to reign in the power of surveillance organizations and limit the scope of national databases. They knew that government would not act to stifle its own increasing power. Even more quagmiring was the fact that the internet was on the verge of its privatization boom (at the time of Zimmerman’s first work on privacy). The government was concerned about pushback from business with which it had partnered for years to built the internet.

Zimmerman responded by creating an email encryption method that is still unbroken. Pretty Good Privacy (PGP) was developed as a technological answer to the question of digital privacy. And when the government tried to deny the right of citizens to use the technology, Zimmerman took them to court. The government did not want to allow powerful methods of encryption that for which they did not already possess “back doors” (Department of State Bureau of Politico-Military Affairs 1993). In fact, the government tried to step in between citizens and privacy by using the appeal of encryption. The Clinton administration repeatedly created campaigns to co-create computer chips that would handle encryption for people and devices. For people, the purported benefit would be encryption. For the government, the benefit was a known backdoor in every sign chip produced. During this time period the government popularized the escrow method of encryption key management. If they could not manage a back-door exploit, they would make sure that they possessed a valid encryption key for every chip. In essence, the government pushed for its interpretation of privacy in the online space: governmental cyber security. This is despite the ever clear reality that non-authorized actors were gaining access to government collected data through non-digital means (Hemphill 1974, 596).

Regardless the governments attempts to co-opt encryption and continue to define digital privacy, Zimmerman profoundly concluded that encryption technology was an excellent way to attain digital privacy — his PGP technologies are still unbreakable decades later, but the best technology was that of the mind. People needed to changer their behaviors and social expectations. This is because even if encryption became exploitable, if it remained sufficiently time consuming to carry out, the collective practice of using encryption would dissuade encryption cracking as the primary means of obtaining people’s data. It would also reduce the rush to action which Michael Colaressi claims causes problems with policing and military action in the digital age (2020).

Zimmerman rightfully recognized that “advances in technology will not permit the maintenance of the status quo, as far as privacy is concerned” (Zimmerman 1999, para. 10). He postulated that digital technologies would only allow for greater surveillance and controls by the government. Of the increasing predicament of digital privacy, Zimmerman wrote: “If we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could never have dreamed of" (para. 10).

By 2001, the controversy over encryption technology use by people in the U.S. was cooling down. Partially because legislators were concerned about their own privacy in the online space, but also, because the September 11th attacks refocused security efforts extra-nationally. Also, because the government thought better to pursue more fundamental surveillance powers which would allocate them the funds, technology, time, and purview to access whatever they wanted. The Patriot Act was on the horizon. This effectively ended the discussion about encryption because in most cases under the new powers of surveillance there was no need to ask for access, nor a right to privacy technologically (Patriot Act of 2001).

People of color have always been the target of *neo-surveillance* that was spawned by the rise of computer and networking technologies. This is because people of color, and other minorities, became increasingly interested in communist-socialist theory in the post-war period. Minorities recognized the inadequacies of the current governmental system to provide them with their basic needs. This frightened the federal government. In particular, the FBI played a central role in defining digital privacy for minorities. The agency's interpretation was that there was no afforded privacy to these minorities; this is evidenced by their carte blanche operations. As technologies escaped the government's grip, digital privacy became a reality. Digital privacy at least was correlated to encryption. However, it was soon recognized that social-behavioral norms that were adapted to invasive technologies represented the frontier of digital privacy. Philip Zimmerman was a pioneer of both the technological and social constructions of digital privacy. The encryption technologies he created and the open-source development environment that he fostered are fundamental to an understanding of modern digital privacy. Having only penetrated social consciousness after the turn of the millennium, the concept of an actionable digital privacy is still relatively new.

A New Millennium and the Divided Online Space

The modern digital divide is both a material and socially constructed problem. *Digital divide* was coined in the mid 1990s during the privatization boom of the internet after the introduction of HTML and the World Wide Web technologies. However the term emerged, Manuel Castells (1996, 1997, 1998, 2004) postulated at length about the existence and potential effects of a divide in the online space; this is known to spawn the first order digital divide on access. The second order was theorized by DiMaggio and Hargittai (2001), Rogers (2001), Selwyn (2004), and van Djik (2005) who critiqued that access inaccurately framed the problems of people and the online space. Instead, these theorists borrow from literacy theory and argue that skill differences bifurcate the online space and create the digital divide. Lastly, there exists a third order where social and communal factors effect the “opportunities of meaningful use” by individuals (Warschauer 2003; Hilbert 2011; Moussa and Seraphim 2017). Ritzhaupt, Liu, Dawson, and Barron (2013) explain the third level as whether “users know how to use information and communication technology (ICT) for their personal empowerment”. This section of the literature review will delve deeper into the digital divide as it pertains to minorities. It reveals that, while much work has been done to close the digital divide gap for minorities when it comes to access and skills, much more research needs to be done on the social influences of online access and use.

Initially, the digital divide was theorized as a small-t theory. Politicians of color and community members asserted the digital divide as a racial one. However, through the National Telecommunication and Information Administration's research, significant challenges to the theory of digital divide as simply racial arose (National Telecommunications and Information Administration 1999). Jæger (2004) analyzes two elderly internet access programs to identify elderly populations as valid members of "the information society" (14); O'Neil and Baker (2003) take a similar approach in their assessment of "successful" family technology resource center programs in impoverished communities in Atlanta, Georgia. Liff and Shepherd (2004) examine the digital divide as a gender-based one, and Payton (2003) introduces sexual minorities to the divide, along with intersecting race and gender: African-American women. Zhang and Wolff (2003) expand the digital divide to encompass the urban-rural spacial divide. The particular physical requirements of computers and the internet prompted Solomon (2000) to confront the digital divide from the perspective of persons with disabilities and create the "disability divide". Dobransky and Hargittai (2006) extend Solomon's work by examining usage cases amongst persons with disabilities and the financial predicament in obtaining at-home access. Although all of these inquiries into the digital divide are founded on the assumption of the divide being one of material access, there are hints that the researchers recognized that skills differences represented a more complex problem despite access becoming more widespread (Payton 2003; O'Neil and Baker 2003, 308-311; Jaeger 2004).

DiMaggio and Hargittai (2001), while acknowledging fully the substantial digital access divide, refocus the debate on a skills perspective: "what are [people] *able* to do, when they go on-line" (4, emphasis in original). They also expanded the definition of the internet beyond simply the hardware it runs on; instead, they argue for including the structures that result in the implementation of the online space: profit-seeking corporations, government agencies, and non-governmental organizations (4). DiMaggio and Hargittai challenge early dreams of an internet that spawns self-learning because of access (Licklider 1965). If anything, they reinforce later perspectives expressed by Licklider and Taylor(1968) and Lederberg (1978, 1317) on the possibilities of technology becoming less understandable to everyday users as time goes on. Goedhart, Breorse, Kattouw, and Dedding (2019) echo this message in their focus on the digital divide as it affects immigrant mothers in Europe. In their study, they observe that incomplete ICT skills can negatively impact a mother’s usage of online communication despite having access, and the negative impacts can then extend to their children who are tasked with facilitating access. The skills divide between the mothers and their children upends the normal social dynamics between them. Geodhart, Breorse, Kattow, and Dedding demand that internet access programs include skills training, especially for vulnerable populations. Reisdorf and Rikard (2018) extend that argument to prisoners. They find that prisoners are not being equipped with the necessary skills to access the online space. This lag in digital skills can negatively impact recidivism, and thus, they argue for a “digital rehabilitation” where prisoners will be trained on the hard and soft skills of the internet to help them reintegrate into society. Skill inequalities are a huge issue and represent a large portion of the modern digital divide (van Deursen and van Djik 2011). The prevalence of the second-order digital divide is the result of an online space that is increasingly reliant on evermore complex technologies. Contrary to Licklider’s initial prediction that computers would help us make more sense of the world, digital technologies seem to have the opposite effect.

The third order of the digital divide focuses on the online-offline social dynamic that influences internet use despite equal access and skill. Mehra, Merkel, and Bishop (2004) argue that conventional quantitative research on the digital divide is important and helpful, but they assert the importance of understanding the digital divide from the human perspective, "to understand the scruffy realities of marginalization in which internet use is embedded, the complex intertwining of sweeping socioeconomic processes and power dynamics with harsh everyday realities" (782). Their research looks at the use of online space by low-income persons, sexual minorities, and African-American women for self-actualization. Foley (2004) examines how access can help overcome offline social exclusion, while Schradie (2011) examines how the divide manifests different online cultures by examining the *digital production gap*.

The digital divide is still predominantly thought of as an issue of access, and there is much truth to this conceptualization. There are many people living in rural communities that still lack access or use subpar service. This includes many native people's living on reservations in the U.S. (S. HRG. 116-116, 2019). However much research currently focuses on examining skills and social gaps in the online space in order to explain the persistence of a division between those who participate in the online space. The perspective of the digital divide has also changed. Instead of simply viewing the divide as the symptom of material and social problems, theorists are now examining the divide through a lens of causation; it is both the result of and influences social norms, economic trends, and culture in the offline space.

Urban Illinois Areas & the Digital Divide

Although Illinois is thought of as a high access state (at the time of writing, according to *broadbandnow.com*, which reports statistics on broadband internet access, Illinois has the 6th best broadband coverage), issues with equal access have warranted a reassessment of how the state is dealing with the digital divide (Taglang 2020). Covid-19 has also spawned a rethinking of what is meaningful access. Assuming widespread meaningful access because of the proliferation of mobile phones with data plans is unhelpful. Are students expected to use Zoom, take notes, and consult sources all on the same 6.5 inch device? Even before Covid-19, the state of Illinois announced a program to rethink the access divide (Hansen 2020). The first studies were set to begin in early 2020, but that progress is likely upended by working from home because those who were the foci of the research are thought to have no or slow internet connections. What is clear is that rural and some urban areas have a lack of access, and if they have access the service is substandard.

Access is even more complicated than previously thought because of where access is attained. Many urban and rural students attain access by going to school or having access to a library. They may not be utilizing the internet at home despite a wired connection coming directly to their building. Some of the confusion over access results from the non-standard ways of delivering internet service — to the neighborhood, to the building, or to the node.

When it comes to digital skill attainment, the Chicago Public Schools system introduced programs quickly after the turn of the millennium (Consortium on Chicago School Research 2007). The programs which were paired with new infrastructure are seen to be successful, but there is no way to know what level of user ability was attained by students or parents exposed to the programs. There have been similar programs conducted downstate at universities and libraries. These are areas that need further study. However, they are outside the scope and focus of this research.

Why not Cyber Security?

The online space's inception as a weapon of espionage impacts how stewards and users of the internet conceptualize safety. The foremost safety in the online space is found within cybersecurity theory which derives from traditional security theory. In the context of virtual privacy networks (VPN), Norton — one of the largest sellers of online protection tools, differentiates privacy as a means of "block[ing] websites, internet browsers, cable companies, and internet service providers from tracking your information and your browser history" and security as something which "helps protect you from other people accessing your personal information and other data" (Gervais 2020). The differentiation of privacy as safety from companies and institutions and security as safety from other online actors is faulty. Even by notions definition of privacy, privacy would be included within security. By separating the two, it merely separates out those whom Norton, and many others in the industry, are comfortable assigning as manageable agents in the online space. The privacy-security bifurcation also mimics traditional notions of safety found within the national security framework. This section of the literature review explores the origin and operationalization of cybersecurity theory to highlight the lack of security perspectives that compensate for the conceptualization of online safety as privacy.

Since the beginning of the internet, the online space has been conceived as securitizing and securitized. Initially, “internetworking”, how people referred to connected computers before *the internet* became the standard term, was a means of executing particular security endeavors. In its capacity as a tool, it was securitizing. Subsequently, the internet became an online space that was perceived to be secure to the extent that valuable communication and research could be conducted within it. Thus, the internet itself became securitized. With the privatization and rapid expansion of the online space, that perception of the internet as secure has waned. Now, the perception is the online space in anarchical with bastions of security. In other words the online space is a microcosm, or exocosm, of the international community. For this reason, it is valid to draw parallels between security in the international context and cybersecurity — especially since national security was the impetus for the internet.

Traditional security, as a responsibility and a power, is abdicated upward from individuals to institutions. The highest institutional layer is the nation-state and thus the state wields unimaginable responsibility and power when it comes to security, usually of maintaining borders and preventing invasion. From the traditional security perspective, material factors are the primary determinants of preventing harm by an external actor or action (Buckley 1987; Buzan 1991; Levy 1995). This perspective of security comes directly from warfare strategy and dominated until the collapse of the U.S.S.R.; it "emphasizes military threats and the need for strong counters", status quo orientation, and the centrality of the state (Booth 1991). Cybersecurity adopts this same framework for assigning power, identifying manageable agents, and formulating tactics. Private companies which dominate the cybersecurity and the public institutions that hire them have focused on centralized solutions that rely on expansive technological integration and superlative power: remote servers, firewalls, encryption. Cybersecurity operationalized in this way completely removes the ability of an individual to participate in the security process.

Controversially, the traditional security approach has led to many high-profile cases of data breach (Fuller 2019). Cowley and Perlroth write about the cybersecurity strategies at various financial institutions: "MasterCard, for example, has a windowless bunker at its data center in Missouri, where a group of security experts work. Citigroup runs three cyberattack response centers - in Budapest, New York and Singapore - that give it round-the-clock coverage. JPMorgan Chase spends nearly $600 million a year on security, and Bank of America's chief executive has said the bank's security team has a ‘blank check’ for its spending" (Cowley and Perlroth 2019).

Appropriating Fuller's term, the immense investment born out of realist notions of security have been ineffective in combatting *cyberinsecurity* (Amir, Levi, and Tsafrir 2018; Talesh 2017). Just as with the military industrial complex, there is a vicious cycle that is promoting security behavior which has not realized an actual benefit to individuals but has the positive externality of making a lot of people wealthy.

One contributing factor to the increase in cyberinsecurity is the growing amount of information that is being shared purposefully or inadvertently by individuals with institutions. Norton's official site identifies the unnoticed movement of individuals' data beyond the initial institution which gathered it as a breach of privacy despite it not being a breach of security (Gervais 2020). This shows that there is a unexplored aspect of safety in the online space which could potentially yield great benefit, but there is a disincentive to explore it because doing so would disrupt the status quo of individuals relinquishing information to institutions. Taking into consideration the preference of the aforementioned in theorizing security, this thesis centers individuals instead of institutions, and therefore focuses on digital privacy instead.

As an aside, I advocate for the use of the term *safety* instead of *privacy* or *security*. Because privacy focuses on addressing weaknesses to exploitation by institutions and security for other users, they do not fully capture the predicament of people of color in the online space. People of color are not simply in danger of exploitation by one or the other, they are potentially violated in the online space by systems, institutions, and other persons all at the same time. Furthermore, security is not effective when trying to understand the perceptions and motivations of individuals because security technologies in the online space are increasingly unavailable to individuals, the hardware is expensive and the technologies are difficult to implement and maintain. And privacy does not capture the stakes for people of color in the online environment. They are not simply trying to keep something unviewable or unknowable for trivial or financial reasons. Increasingly, they are put in potentially dangerous situations because of their exploitation and exposure in the online environment. People of color in the online environment are looking to attain and maintain the human right of safety in the online space, and in many cases, it is substantially challenged.

Theories of Digital Privacy

Because this study examines digital privacy strategies as they are affected by a racial digital divide, I use a justice framework on digital privacy developed by Ashworth and Free (2006) to make sense of participants privacy protection motivations. They formulate a justice theory of digital privacy which identifies two main components to perceptions of privacy in the online environment: distributive and procedural justice. Distributive justice is characterized by "a perceived fairness of the allocation of outcomes and is assumed to reflect a concern for one's material well-being" (113); thought, there is a distinction between what is seen as fair and what is seen as advantageous (114). Procedural justice is the perception that decision making within a group has involved members to "the extent that it communicates to relevant individuals that they are valued and respected members of the organization" (113). Within procedural justice, openness, information access, permission, and honesty are foundational. When companies do not meet the expectations of online users in regards to three areas, the sense of procedural justice dissolves (116). Without distributive or procedural justice, people in the online space feel that their privacy has been violated and seek recourse.

To understand people's behavior after they feel that their privacy has been compromised, I appropriate the privacy behavioral model developed by Chen, Beaudoin, and Hong (2016). They have identified four behavioral categories rooted in risk avoidance behavioral theories of approach and avoidance (Piko 2001; Youn 2009): privacy setting, contact management, access setting, and identity masking (Chen, Beaudoin, Hong 2016, 418). Privacy setting involves clearing or limiting one's digital footprint via actions "such as clearing cookies and browser history, encrypting communication, deleting previous postings, and avoiding websites that ask for a real name" (418). Contact Management is when the user blocks users they have already become friends with, refuse friend or follow requests, and ask others to take down content which features them. Access setting restricts "sensitive" content to trusted members of an online community, and lastly, Identity masking is using an alias to conceal oneself from organizations, companies, and other users.

The objective of this research is to investigate how the digital divide affects perceptions of justice in the online space and how those different perceptions of justice result in variance in digital privacy behaviors amongst urban minorities. I examine from the perspective elaborated in the literature review; the internet has and continues to be a dangerous space for urban minorities. The primary use of the online space has been for surveillance and oppression of urban minorities. The current public sentiment of an internet of freedom and expressivity contrasts greatly with that of the government. This can be seen in agency actions, legislative efforts, and legislator spawned discourse on the internet, security, and privacy.

As a note, there are two pandemics that currently affect this research: the global Covid-19 pandemic, which began in January of 2020, and the pandemic of racism that persists in this country. The global Covid-19 pandemic has already claimed the lives of more than six-hundred thousand persons, with no end in sight. There are almost fifteen million infected, and the number continues to rise. In the U.S. specifically, we are nearing one-hundred thousand new cases daily. For the racial pandemic, there also does not seem to be an end in sight. Most recently the nationwide George Floyd and Breonna Taylor protests spread from large cities to even the most intolerant crevices of our country. Notably, thousands marched on Washington D.C. to let the forty-fifth President of the United States, Donald Trump, know that they will not stand for the unjust police killings against people of color in this country. These pandemics have been ongoing during the period of research and undeniably impact how people are perceiving the world and themselves. Although it was not initially my intent to explore digital privacy during a moment where more people than ever in the history of the Anthropocene were spending their days in the online space (because of Covid-19 work from home); although it was not my intention to investigate digital privacy during a moment where the President of the United States, himself, commits COINTEL-

PRO like actions from his office by posting pictures of protestors on his official twitter account; this is the current reality.

CHAPTER III: METHODOLOGY

Method/Design

This research explores the perceptions of justice in the online environment by people of color and examines how those perceptions influence the use of specific digital privacy behaviors: privacy setting, contact management, access setting, and identity masking (Chen, Beaudoin, Hong 2016, 418). To understand how participants perceive justice and determine their use of digital privacy behaviors, the study employs three anthropological methods: semi-structured interviews, a "profile-eliciation" exercise (Mannik and McGarry 2017, 179-195), and auto-ethnography (160-178). The semi-structured interview includes eleven questions. The first question was consent to record, and the latter ten questions were open-ended questions asking about privacy and their online behavior (see Appendix A). The "profile elicitation" involved showing four faux social media profiles to the participants and asking them to note any differences they notice in relation to the data displayed or privacy features they think are enabled. Lastly, the auto-ethnography involved asking the participant to write a short-essay about themselves from the third-person perspective. I also talked to people who were not formal participants in the study.

Participants/Procedure

The researcher sent a university-wide email to all undergraduate and graduate students to inform potential participants of the research study. In addition, study information was disseminated on the researcher's personal and professional social media profiles. The email included the research information and contact for the primary researchers. Current and former students who were interested in participating would email the primary researchers and in return would be sent a detailed study flyer and informed consent agreement. The study flyer and the informed consent communicated the breadth of the study and students' rights during the process. The study was approved by Illinois State University's Institutional Review Board. This study was qualitative and therefore allowed for more full responses from participants. Because of the variance in questioning, including self-questioning, the design allows for the researchers to understand and cross-check the responses of the participants. Of the seventeen formal participants in the study, half I recruited from my personal and professional social media networks. Four knew me in my day-to-day life.

Measures/Analysis

The semi-structured interview was broken into three parts. The first allowed the participants to provide demographic information, their own perceptions of urban minority, and to conceptualize privacy on the spot. The next section asked them specifically about the digital privacy strategies that they have employed. The last section asked them a range of questions about social media profiles and privacy. A coding scheme was developed and applied based on the theory of digital privacy strategies to look for specific terms that signal behaviors. This data was analysed with a more open ended approach, and provides context to the coding method applied in the semi-structure interview. For the auto-ethnography, the participants essays are coded using behaviors they have expressed in the semi-structured interview as unsafe. In addition to the controlled research, participative observation as part of the researchers everyday life in the digital environment.

CHAPTER IV: THE WHITE SPACE

Tyga & Crocheting While Black

Tyga is a millennial woman of color from the south side of the city of Chicago. She is mixed-race Black and white, but she identifies as Black and is a member of the Black community. She recently obtained her bachelor's degree. Tyga is an avid crocheter who thinks of crochet as a therapeutic practice. She went online to find the broader crochet community with whom to share experiences and ideas. When we discussed her personal feelings of safety in the online space, she spoke of experiences that are constant reminders of the presence of her oppressors. When asked, how safe she feels in the online environment, Tyga responded:

> On a scale from one to ten, I probably feel like a four or five…I just know that as a Black person that we are heavily surveilled, and I'm like very much a part of the fiber community, crochet community, and seeing how Black people posting in an outfit that they've created will get censored and blocked. And someone from a different race, or someone who identifies as white or perceived as white, they weren't getting the same kind of surveillance. So, I feel that I have to be careful of the content that I post, my political messages and censoring myself because I don't want to garner attention.

Tyga continued by mentioning a big name in the fiber community, a woman of color, who was censored for wearing crochet shorts while white women wearing similar garments were not.

> It was censored. The picture was taken down from her profile, and the tags that she had associated with the top were all blocked…Even all the pictures that weren't hers, where people used the tag, they were removed too.

Tyga made sure that she was careful about what she posts online in fiber communities after witnessing this situation unfold. Later in the conversation, Tyga clarified that she was even wary of posting pictures of patterns that used designs that could be perceived as ethnic or expressing ethnic pride because she fears persecution.

When asked if Tyga thought it was the platform's internal review processes or other users individual reporting that resulted in the censoring of Black crocheters' images, she explained that, to her knowledge, the fiber community was divided, and a culture of reporting Black content had arisen. She cites the election of President Donald Trump as a huge impetus for this rift.

> They are calling out a lot of racism that exists within the fiber community. So with that, there's been this huge backlash. And a lot of prominent knitters, primarily white knitters who do not want to get with the program, they started making their profiles private. They started creating a colorway [specific dye patterns] that makes fun of the Black Lives Matter movement and people of color. And they will report Black content.

Tyga mostly spoke in our interviews from her perspective as an instagram user, but she also talked about her negative experiences on the Facebook platform. She reported similar forms of harassment on that platform previous to deleting her account. She bemoaned the fact that people were not interested in forming a community; instead, they used the reporting process as a means of suppressing the voices of people of color. Unfortunately, because of the biased review process, the racists, misogynists, and trolls continually won. So, Tyga eventually deleted her account.

Tyga deals with the online dangers that are tied to her Blackness and womanhood by posting selectively [access setting], making her profiles private [contact management], and eventually self-deplatforming [privacy setting]. While she identifies a culture of hatred as the immediate threat, she also reports her fear of the uneven procedural justice for people of color in the online space. The reporting process, which is a foundational system of justice in the online space, was being used by the oppressors to perpetrate attacks against crocheters of color. It is clear that she believes that creators of color’s innocuous content would not be taken down if the reporting process were fair and consistent.

Noshi & the Midnight Massacre

Noshi is a Black queer trans person, an older millennial, and an experienced user in the online space. During our conversations, they spoke extensively of the censoring of Black and queer persons and their content in the online space. They became particularly impassioned when talking about the mass exodus of Tumblr which began in 2013. Tumblr was the refuge of weirdos, sex positive persons, queer persons, anime obsessors — people simply looking for a safe space— for many years. After the purchase of the platform by Yahoo in 2013, the platform announced a radical change in its acceptable content policies. Yahoo sought to “clean up” the platform. At first, Tumblr users were reassured that the target of these new policies would be illegal and inappropriate content only. However, the words and actions of the platform were incongruent. Noshi explains:

> Yahoo was like, okay, we're going to start censoring what people can put on our site…The problem came, in the sense that what they decided to censor was too large of a scope. One of my favorite sayings is ‘we hunt with rifles, not grenades’. They hunted with grenades. They basically decided to just mass censor a lot of content on the site. There was a huge government push against sex work and pornography and things like that. So like, they became way too serious about censorship. They were very serious about censoring, ‘female presenting’ nipples. That was like the quote that stuck out to everyone. So like, once that hit, I left. I left that platform because they started restricting content. They started censoring people's content that wasn't even pornographic, wasn't even nude, wasn't even anything. Literally, [people] went to sleep, and they woke up the next morning. And legitimately, two thirds of their content had been restricted, had either been deleted, or restricted access to it, or just censored so that people would have to go through like a barrier to access it. And I was like, Oh, no, I'm good on that. And I

> left that platform, and I haven't been back. So yeah, that's just one. That's one example of it.

Noshi vividly recounts how the community was attacked by the platform. They were pinned into submission. The platform did not consult the community at all. Noshi’s reason for leaving the platform reveals their concern with procedural justice. When they felt it impossible to attain such justice, they practiced extreme privacy setting by self-deplatforming. They had deemed that there could be no safety found on the platform. As they stated, there was no transparent review process; there was no appeal process; and the actions were done without notice. A majority of Tumblr users at the time, many of whom were queer person-of-color artists and models who created safe spaces on Tumblr, never had a chance to save their content or preserve their profiles. They, like Noshi, fled the platform. For those artists, leaving the platform potentially cost them a great deal: friends, exposure, collaborations, feedback on their work, a history of consistently being active and producing quality work. Many gave up much to self-deplatform. However, they felt that their safety in the online space was worth the cost of leaving the platform.

The White Space According to Anderson

Researchers continue to investigate how offline social organizing and practice affect peoples’ use of the online space. The work of Fuchs and Horak (2008), Morales et al (2016), Kafer (2019), Kania-Lundholm (2019), Wajcman (2015) show that there is no longer a clear offline-online space, and that minority status in the online environment is precarious. Fuchs and Horak conceptualize a *digital apartheid* by examining the digital divide on the African continent. Starting from their assertion of digital apartheid, I work backwards using Elijah Anderson's *White Space* framework to understand the online space, digital divide, and minority participation in the U.S. context. Investigating the racial elements of digital inequality has mostly been taboo in the West. Digital inequality has mainly been framed as a socio-economic issue but not a racial one. The accepted research norm has long been that digital disparities may align with racial divisions, but the effect of race on digital inequality is overstated. The lauded Johannes van Djik, in partnership with Kenneth Hacker, (2003) wrote in a quantitative investigation of the digital divide that "talk about 'technological segregation' ([by] NAACP President Kweisi Mfume) and 'classical apartheid' ([by] Reverend Jesse Jackson) is exaggerated and misses the point" (324). Almost two decades later, the interest in digital inequality as it relates to race and ethnicity is rising, mainly spawned by global south theorists and activists, and the dismissal of Mfume and Jackson's words appears misplaced and irresponsible.

Anderson (2015) defines white space — settings in which Black people are typically absent, not expected, or marginalized when present (10) — and identifies three factors that contribute to the maintenance of a (physical) white space: policing, gentrification, and outright violence. I apply these criteria to explain that the online space is white space and that the conceptualization of the digital divide as racial is sufficiently valid. Before we move into the theory and cases, I emphatically agree with Anderson's conceptualization of white as white-passing and Black as not white-passing.

Anderson argued that white people create spaces where they feel comfortable foremost via policing. In the case of outdoor space, this is mostly literal physical mechanisms to remove Black persons and put them in their rightful place, akin to slave catching. There are countless cases of Black persons being surveilled by white people and having the policed called on them (McNamarah 2019). One such case was that of 43 year-old Travis Miller Senior. Travis works as a furniture delivery driver in the Oklahoma City area. After he delivered furniture to a home in a gated community, Travis was followed by a white man who suspected him of being a burglar. The white man then blocked the road with his car to disallow Travis and his coworker from leaving the gated community grounds (Padilla 2020). As Travis tried to reason with the initial white man, the white man called a friend to come and support his attempts to block Travis' truck from leaving. The entire incident was recorded and streamed on Facebook Live. The initial white man who followed and blocked in Travis justified his actions by saying "I own one-eighteenth of what you're sitting on. This street is private. This is not city property. This street is maintained by the people that live in here." (para. 13) The situation was resolved by the resident who order the furniture. And the police, who had been called, were told to stand down. By the end, Travis could be seen breaking down with tears streaming down his face. Similar actions against people of color are perpetrated across the country and reify physical space as white space. The white men were eager to catch a Black man "out of place" so that he may be returned to where he is allowed. While the argument that Travis was a burglar seems plausible at first utterance, is it? Travis is a burglar who knew where the gated community was, gained access to the community, procured a fake uniform, called a fake supervisor, engaged peacefully with people who questioned him about his appropriateness in "their" space, and never tried to run away when confronted, and was leaving the premises with an empty truck?

Common forms of physical policing are: the police, redlining, sundowning, dress policies, hair-style prohibitions, but, if a Black person is physically allowed into a space, policing transforms into social policing. Anderson identifies the " 'dance,' through which individual blacks are required to show that the ghetto stereotypes do not apply to them" (13), as the expectation lest eviction from white space occur, immediately or "in due time" — the dance is also referred to as "walking the tightrope". White people conceive of the ghetto as a place of "danger, crime, and poverty", and actions associated, accurately or inaccurately, with the ghetto trigger a danger response from white people. Common forms of social policing are: using offensive terms to refer to Black people, correcting Black speech, ascribing culpability because of common ethnic outward appearance, prohibition of open-air playing of rap music at residences, in parks, and at events. And, just like in the old days of slave catching, there are consequences for infractions. However, in most cases, the pressure of the white space, which taps into white privilege and power, is implicit, so Black people comply. This results in the yielding of space, and Black space is born again as white.

Secondly, Anderson identifies the inverse action born of white surveillance powers: gentrification. This can also be expressed as a type of appropriation of cultured space. If white people are not scared by the ghetto, they are drawn to it. They invade neighborhoods and transform them through concerted capitalistic actions different from those normally found in working-class Black spaces. This is to be differentiated from white persons simply moving to and participating in Black communities. Usually, those looking to gentrify are looking for specific cultural aspects that are readily commodifiable, and they know that through targeted investments they can refine aspects of the neighborhoods deemed acceptable. They eradicate the rest, including people. Black people living within gentrifying neighborhoods are simply along for the ride, captured in the financial aims of white outsiders and those who are doing the “dance” at the most proficient level.

The last method highlighted by Anderson is outright violence. Anderson borrows the experiences of a law student in Washington D.C. to demonstrate how violence creates white space. Shawn was brutalized by police as he waited for the bus to go home after grocery shopping. He had been doing nothing wrong. He had been waiting with other people. And he was complying — even to the extent that he dropped his phone and groceries. However, he was still brutalized by police. This despite the pleading of those around him. Even if they wanted him to feel safe and included in the space, they had no power to change the reality that the act of brutalizing would have: creating white space. Shawn’s case is especially disappointing because it demonstrated how all three processes of white space work together. The white people in his neighborhood had surveilled him, deemed him suspicious, and reported his description to the police for a robbery. While the actions of the neighbors was wrong enough, it was the violence against Shawn’s Black body which was witnessed by white people in the neighborhood which created the white space. Those who disagreed with the actions of the police were powerless to stop its effects, and those who thought the violence justified felt vindicated. Shawn’s experiences mirror my own of being arrested, roughed up, and detained by Madison, Wisconsin police as a seven-year-old.

The vignette of police brutalizing Shawn, a law student in Washington D.C., serves as a reminder of the most often used method to achieve white space: violence. The Colfax, Louisiana Massacre 1873; Wilmington, North Carolina Massacre 1898; Wounded Knee Massacre 1890; Atlanta, Georgia Massacre, 1906; East St. Louis, Missouri Massacre 1917; Elaine, Arkansas

Massacre 1919; Tulsa, Oklahoma Massacre 1921; Rosewood, Florida Massacre 1923; Catcher, Arkansas Massacre 1923; Ponce, Puerto Rico Massacre 1937; Chicago Memorial Day Massacre 1937; Orangeburg, South Carolina Massacre 1968; Greensboro, North Carolina Massacre 1979; Oak Creek, Wisconsin Massacre 2012; and the Charleston, North Carolina Massacre 2015 are also testament to the extent of violence that has been acceptable against Black persons for the creation or maintenance of white space.

Applying Anderson's framework, we can assess the online space to identify instances which would reinforce it as divided on racial lines. First, let's look for policing. Maarten Sap et al. (2019), Davidson, Bhattacharya, and Weber (2019), and Guynn (2020) demonstrate that Black people's posts are flagged more often because their vernacular is deemed "offensive" by white users and AI. Those that are supposed to be helped by the system end up being policed by it. And users engage in the same policing behaviors as platforms to the detriment of Blacks in the online space — as my participants experiences will show. A 2015 Wired Special Issue article by Bijian Stephen shows how Black space even at the beginning of the Black Lives Matter movement was contested. The interviewed activists explain that they felt watched in the online space and expressed an effort to explore alternative to the major platforms. Years later, a Washington Post article by Antonia Noori Farzan exposed police infiltration of Black Lives Matter Groups (2018). No one knows the exact scope of these operations or how much control was and is asserted over the spaces that are thought to be safe for Black people (Loedenthal 2014).

Gentrification in the online environment is a regular occurrence across all social media platforms. It is most often criticized as simply appropriation, but this wording ignores the insidiousness of the action. In the context of the cut-throat online environment, a white person appear-ing on instagram doing traditional Black hairstyles will inevitably destroy the existing or potential viewership base for Black persons. There is no dominant term for this action, but the term “blackfishing” has been used by some in the online space. The most egregious example of blackfishing, which alludes to catfishing — defined by Oxford as luring someone into a relationship by means of a fictional online persona — is the Kardashian family. Besides the fact that most of the Kardashian women have drastically altered their appearances to look more Black, they have used blackfishing to authoritatively appropriate Black styling and hairstyling techniques. Most notoriously, Kendall Jenner was strongly criticized in 2018 for wearing cornrows and receiving credit from fashion magazines for the “new styles”. She also credited the style to Bo Derek and completely erases their African-American roots by referring to them as “Bo Derek Braids”. As many people of color on social media rightfully reminded fashion magazine photographers, columnists, and readers, the entire Kardashian family has become rich and famous by stealing from other cultures, and they rarely publicly address social justice. They wear cornrows for a fashion shoot to look edgy, but say nothing of the discrimination of Blacks for wearing the hairstyle. White people are assuming the bodies of Black people, literally replacing them in the online space (Virk and McGregor 2018; Jackson 2018).

In another example, Rachel Dolezal masqueraded as a Black woman for much of her adult life, becoming a professor and activist by appropriating Black struggle. Even after being “outed” in 2017, she continues to insist that she is not white and that she identifies as Black (St. Felix 2018; Levine 2020). A similar situation unfolded in late 2020. George Washington University professor Jessica Krug “came out" as a white woman (Jackson 2020). She had already received funding from organizations that were seeking to support Black women in academia (Flaherty 2020). In a more insidious manner, these white women adopted Blackness and found success. Criminal or not, their actions marginalized Black women. In the online space, it is even easier to assume darker skin and kinky hair because of social media filters that darken skin, add hair, and apply make-up; white people have been creative in the use of these technologies not merely for entertainment but for profit and power.

Lastly, violence directed towards Black people happens in the online space. If anyone has ever played an online game, they have experienced it. As soon as you connect to the matchmaking lobby, someone screams “nigger”, “beaner” or “faggot”. The online gaming world is usually wild but sometimes it goes beyond being bombarded with slurs. Even without the clear intent of the speaker, it is undeniable that events like this hurt people of color and make them feel unwelcome, whether they are prepared for it or not. In some cases, it’s not so immediate, and the violence occurs during moments of high pressure in the online environment, or sometimes for no reason at all (Sholars 2017). It is not uncommon for groups to form for the sole purpose of antagonizing gamers of color. Some groups will only attack players who have Black in-game characters, user avatars, or names that sound Black or ethnic (Castro 2019; Pettit 2020; Van DerWerff 2014; Alford 2020; Miller 2018).

Outside of gaming, harassment is widespread on big social media platforms. In 2020, a Facebook Blackout day was organized to force Facebook to address harassment of Black people on the platform (Guynn 2020); it was moderately successful, but there was no major action by Facebook although there were perfunctory statements by the platform.

With Covid-19 restrictions and the rise of working/school from home emerged a wave of “Zoom-bombing” that were suspected and known to be racially driven (Bond 2020). These hackers, or moderately savvy internet users, interrupted meetings held via the Zoom video conferencing software. They targeted events by Black people and showed hurtful images and screamed hate-speech — the bowels of the internet, 4chan, planned it openly (Bakht 2020).

Using Anderson's framework for the white space, we can identify similar methods of policing, gentrifying, and violence against Black people in the online space. The online space is often thought of as a utopia, but the days of online anonymity are over and the risks are very real for people of color. The following personal experiences from this study's participants carry the mark of the trifecta of white space genesis, but they most strongly speak about policing.

Many of this study's participants entered into the online environment to derive some social benefit — to find community, to keep in touch with their family. However, after some time they realized that the online space would also deny them privacy. They would not find distributive or procedural justice on big social media. This denial of ownership and privacy emerges from the fact that the online space is purposefully white space, as explained in the literature review, and encourages behavior by white people that maintains the space as white as posited by Anderson.

Ery Explains Systemic White Space

Ery, a queer non-binary millennial of color, also expressed concern at the uneven procedural justice in the online space. Ery is all about justice in their daily life. Social, political, economic, environmental. They talk *the talk*, and they don't endlessly equivocate like most people; they live out their espoused beliefs on making the world a better place. During the course of the interview we talked about the dangers that both people and institutions pose to each others' privacy. In response to this, I asked Ery, “Do you think the bigger threat is the individuals or institutions?”

> I mean, knowing that individuals ultimately make up these institutions and are the ones that have to institute the checks and balances. I mean, even in the instances where people have been posting about racism or use particular words and know that if their content was flagged, it would just be removed. But in other instances where like hate language is being used, posted by someone who's probably like not a minority. Their posts aren't removed this quickly and just knowing that there is some sort of discernment about what gets taken down and when, until, like, the reaction to things that are considered hateful or negative? And who was making that call? As far as I know, it's not an algorithm. I feel like people actually have to look and read these things and make this decision.

Ery highlights that there are a different set of standard and rules when it comes to people of color in the online space. In this case, again, specifically when it comes to reporting and content screening. Ery talks about a long running practice of Facebook moderators to flag posts by persons of color that use offensive language for the purposes of advocacy, education, and empowerment. These posts are usually taken down very quickly. Conversely, posts by non-persons of color, which feature the same words, are not flagged and taken down. In many instances, these posts are not even removed after being reported by users. Ery elaborates that it goes beyond the people who are making the decisions at institutions such as Facebook.

> I wouldn't say that any institution or process is immune from systemic racism and like, the standard of white supremacy in this country, like, we make these tools that we use and we are inherently having those biases and haven’t challenged them well enough for me to be confident that these policing measures [by platforms] are applied equitable.

Ery’s worries about their ability to receive or wrestle procedural justice from the claws of major institutions leads them to post very selectively in the online space [access setting]. Although they have not left any platform, they have chosen to focus on consumption of content they have curated themselves instead of posting. While Ery does not self-deplatform, they do employ a form of extreme privacy setting which they believe provides the maximum safety in the online space.

Anha, the New Challenger

Anha is younger than what is generally considered millennial; she is most likely a member of Generation Z. She is biracial Japanese and White. While she does not readily deem herself a person of color, she does identify with being a minority. She spends a lot of her time on the internet going between the major platforms and social media phone apps, such as Tik Tok. Anha explains, almost impartially, that she encounters offensive content in the online space and tries to report it as much as she can. And although she has had some minor success — she has gotten posts removed on twitter, she says that the majority of the time nothing happens. The platforms investigate the posts she reports, but there is no action. The inaction by platforms confuses her because, according to her, the content she reports is clearly against the rules of the platform. I asked Anha if she felt empowered in the online space and she said that outside of the few successes she has had in reporting content, she does not feel empowered as a user to create positive change on the platforms she uses via the reporting function.

The Author's Personal Experiences

These experiences above mirrored my own experience of reporting someone during the 2020 George Floyd and Breonna Taylor protests. An acquittance of mine, who I met through a group for people preparing to teach English in Japan and those returning from teaching in Japan, started to post racially inflammatory content on Instagram. He was angered by the Instagram Blackout campaign — a campaign where allies to the Black Lives Matter cause changed their profile pictures to an all Black photo and posted a Black square to their profile with the aim of highlight ing Black voices. After a few days, he deleted all of his Instagram photos: pictures of his family, his work, and his travels around the world. Most notably, he deleted pictures of his performances; he was a musician. Soon after his profile went blank, he started to post videos of himself at a shooting range firing large weapons. The tags on these posts usually read something like "They are not going to catch me off guard" or "I'm making sure I'm ready". Previous to this behavior, this acquaintance had gotten into arguments with friends of mine in the comments of my Facebook posts. He challenged that racial discrimination was still an issue in modern society. He didn't understand why people were talking about slavery when it happened so long ago, and there was no one alive who has been a perpetrator or a victim. I had blocked him, but because of the Facebook friend import system between Facebook and Instagram, he was still my friend on Instagram. He previously refused to engage in respectful dialogue but felt entitled to be heard, he never seemed violent. But after seeing the videos, I became worried, so I decided to report the videos. One month later, Instagram messaged me that the investigations into his posts had been closed and that no further action would be taken; there was nothing wrong with his posts. Even considering the second amendment and his right to post on social media, the inquiry and "action" by Instagram took weeks. However, posts about police brutality against Black persons by myself and friends are reported and removed in a matter of hours. Our posts were taken down promptly, but the review of my former acquaintances' inflammatory and violence-inducing posts took over a month.

Hione Stands Her Ground

Hione falls at the tail end of Generation X. She is an intrepid immigrant from Japan who fell in love with her military sweetheart and immigrated to the U.S. She has lived here for 20 years. She is calm yet gutsy. She is always rooting for and fighting for the underdog. She is a teacher that is especially passionate about teaching students with special needs. She loves dogs, and she and her family have rescued many — even right off the street. She has seen hardship and struggle, but she always tries to see the bright side. Many of her posts in the online space are about bringing joy — even during this particularly nasty time. However, that does not mean she shies away from discussions she feels are important.

Hione is not primarily worried about digital privacy outside of her financial safety. She has some concerns about platforms' widespread collection of data and the potential buyers of that data; however, she is not overly concerned because she is, like many other people of color participating in the study, purposeful with what she shares in the online space. This is mostly successful at protecting Hione, but she shared two instances where her presence and participation in the online space was challenged by white men.

In one instance, Hione was engaging in open discussion in the comments section of a major platform. A white men then perused her profile and openly questioned her citizenship. Hione believes that he saw that her birthplace and hometown were in Japan. She explains that the only reason she has these set on Facebook is to be easily found by people that she grew up with in Japan. The discussion was about Japan - U.S. relations, and Hione believes that the man who challenged her citizenship did so purposefully to silence her. She did not back down.

In a second instance, another white man tried to silence Hione because of his suspicion about her national origin and current status. As Hione points out, these actions are purposeful in their use to create white space. The posts on which Hione commented were public and open to all seeking to join discussion. However, the white men felt that an Asian person had no rightful place in the discussion. They assume that being Asian means that she is other. They assume she is not here legally. They assume that being Asian means she uninformed. They assume she lacks the patriotic spirit they associate distinctly with whiteness and maleness. They attacked Hione to drive her away and create white space; if they had their way, she would get no seat at the table.

Justice in the White Space

The experiences provide a personal perspective of how white space is created and reified both structurally and socially. Older people of color participants have a keen sense that they are being watched, and that distributive nor procedural justice is equally applied to them. Tyga and Noshi strongly allude to widespread gentrification in the online space, and how Black culture and creation is becoming ubiquitous and profitable. If people of color (called Black in Anderson's framework) creators and artists are purposefully targeted by platforms, the spaces they previously occupied will be yielded to white persons. This includes the potential economic benefits to be gained by participating in those spaces. This includes the potential say in how the online space evolves going forward. In cases where white people cannot easily police and coop spaces, they will practice violence, such as the coordinated reporting practices explained by Tyga and the attacks on Hione. The experiences of my participants give validity to the thought that the online space is white space. The legacy of the online environment remains unchanged, and that legacy impacts people of color's safety.

The exception within the experiences above is Anha. She is not an older millennial; she is not a millennial at all. However, she expresses an obligation to use her power on the platforms she visits daily. She has some sense of procedural justice. Interestingly, Anha's understanding of her rights and role in the online environment come partly from from her education. As part of the interview, she talked about courses she took in high school which helped her see the digital environment more clearly and prepared her for staking out a safe space. This is potentially the key to surviving and possibly altering the continually oppressive legacy of the online space. It might be the way to disrupt white space for both white and Black users and bridge the divide.

CHAPTER V: INTERGENERATIONAL BLACK TRAUMA

Noshi & The Black Household Noshi

Noshi spends countless hours on instagram and twitter. They are constantly liking and posting about beautiful big Black women, chatting with trusted friends, and video chatting while watching movies and TV shows. They are an avid cuber, a person who solves Rubik's cubes, and an unabashed connoisseur of cannabis. They stream videos of themself cubing while "having a trip" multiple times a week. Observing Noshi in the online space, one would not think that they worried much about privacy, but our discussions and time together in the online space revealed a deep concern about privacy.

Noshi was an eager participant in the study. At the time, they were dealing with suppression of their posts on instagram — their posts were being reported constantly and swiftly removed. I believe this study provided them an outlet for their frustration at what they felt was unfair treatment. After the initial interview, Noshi and I engaged in many discussions about digital privacy and existing in the online space as a person of color. The following paragraphs draw from both the formal interview and many subsequent conversations.

Noshi grew up in a middle class Black household on the far south side of Chicago. When describing their upbringing, they admit they grew up in a home where technology was ubiquitous. By their teen years, they were already becoming concerned and testing the limits of security in the online environment. Noshi specifically cites their ability to conduct penetration testing, which is a fairly involved process that reveals the vulnerabilities of the internet configuration of other online users. While they believe their early exposure to these techniques and technologies influence their current perception and practice of digital privacy, they reveal that their upbringing in a Black household, specifically, has done much to shape their perception and practice. Noshi first alludes to the influence of the *Black household* on their privacy when talking about the sense of freedom and ownership in the Black household.

> Noshi: "So yeah, I feel like the internet is kind of always been through and through [a constant in] my life. I've never felt like it was restricted to me at all or that my privacy was a thing. My privacy existed, like I used to have a journal when I was a kid that I used to write in, like a physical piece of paper journal. And to me, that was like the only private thing that I had. I very quickly realized that it wasn't private because I shared a room with a sibling, and that I had parents. And if you know anything about our households, you know, there's no such thing as a locked door in ***our*** household."
>
> Denavious: "[For those who don't know,] What do you mean by ***our*** households?"
>
> Noshi: "A Black household? A ***Black household*** does not have locked doors!…In a Black household, there's no such thing as a locked door. You don't own your room. You don't have a room. Like, 'Get out of my room!', that doesn't exist in Black households. There's no 'Don't touch my things!'. You don't own anything in a Black household because you didn't pay for none of it. And your parents, at least my parents, were very eager and very willing to inform me and demonstrate to me how much I didn't own anything. So, privacy is never a thing in a Black household. You grow up in a Black household, you're lucky if you have a parent that understands and respects your privacy or the idea of privacy."

For Noshi, personal privacy is founded on notions of personal freedom and personal ownership. Black participants in this study reveal that intergenerational trauma is integral to their formations of privacy and association of justice with privacy; Additionally, it seems that intergenerational trauma guides them to initially preface ownership and, therefore, distributive justice when constructing and asserting privacy in the online environment. After realizing the complexity and impossibility of maintaining privacy on the basis of distributive justice, some Black participants seek procedural justice. However, uneven systemic forces in the online space, which fall on the seemingly indissoluble racial divide, quagmire their efforts. Some participants resort to privacy setting, one of four main digital privacy strategies, to an extreme extent; they self-de-platform.

The vector of privacy, justice, and employed digital privacy strategy is based on a linguistic ideology founded on the construction of a Black household by participants. Black participants in this study either talk directly about or allude to a uniquely Black upbringing. To directly reference this uniquely Black upbringing, they use “Black household”, “our household”, “Black parents”. However, they reference this upbringing in more nuanced ways in the way in which they talk about their upbringings. Notably, when asked about digital privacy, or disprivacy — a term that I use to signify the absence of privacy — many participants reflect on their upbringings and treatment by their parents. It seems that for Black participants, the Black household is deeply important for how they understand privacy and justice and how they employ digital privacy strategies.

The Black household and intergenerational Black trauma as influencers of digital behavior logically flows from initial theorizing on the digital divide and behavior in the digital space. The most well known theorist of the modern internet’s effect on and magnification of offline culture, Manuel Castells, posited that the existing ills of society would persist in the digital realm. However, in this study, and specifically in this section, I examine the personal understandings and personal lineages of the obfuscating, aloof phrasing of intergenerational Black trauma as some permutation of socio-political-economic-status. By adopting the perspective of my participants, who express the importance of intergenerational Black trauma for formations of privacy, I reframe the discourse such that one must always consider who or what is the oppressor in the online space — those who are the oppressors in the offline space; even the father of the Internet,

J. C. R. Licklider, expressly outlines a usage case for adaptive-learning computer technologies for discriminating and gatekeeping undesirable people, “Your computer will know who is prestigious in your eyes and buffer you from a demanding world” (1968, 39). Intergeneration Black trauma provides a framework which involves the ancestors, both far and near, and the present as it affects the privacy strategies of this study’s Black participants in the online space.

This idea of an inherited behavioral legacy in the Black community is encapsulated as *Post Traumatic Slave Syndrome* by Joy DeGruy (2005), but here I have decided to use the combination of the terms which she uses to explain the “syndrome”. That is because my focus is not on pathologizing but explaining human experience. DeGruy theorizes “transgenerational adaptations associated with the past traumas of slavery and on-going oppression” (135) that result in self-hatred, disdain, and even outright violence between Black people in post-colonial environments. The hypothesis is based on DeGruy’s experiences traveling through Africa in the late 1990s observing people and their communities — both colonized and uncolonized — and her experiences living in America as an African American woman and mother. To endure hundreds of years of cruelly successful domination of Black bodies, to endure constant psychological warfare against Black minds, DeGruy posits that Black persons adopted certain behaviors and beliefs that are laced with the trauma of our ancestors’ experiences (101-104).

Of behavior, DeGruy provides the practice of self-denigration. Blacks almost reflexively denigrate their own community, and their family members are not exempt from this practice. Conversely, DeGruy examples this behavior by providing an anecdote of parents speaking about their children after receiving a compliment about their child’s success from another parent. The white parent unabashedly speaks supportively and proudly of their child. The Black parent quizzically speaks badly of their child. I have also observed this behavior. Most of the people in the conversation perceive it as politeness, but DeGruy rightfully questions why the behavior, and often the expectation, is one-sided. Also, what of the child who may be subjected to these remarks. Does the child recognize or acknowledge these comments as tokens in a game of social bartering? Neither DeGruy nor I believe so.

Of belief, DeGruy highlights the what results in child disempowerment. She calls this vacant esteem. Black children do not believe that they can achieve their dreams; they do not believe they can be or do whatever they aspire. The result is an insidious jealousy of the success of other Blacks. Although I did not grow up in a household where this was a mantra, Many of my peers did, and I witnessed and, participated in countless discussions involving older Black men admonishing youth against being an "uppity nigger". This passes the torch of trauma from generation to generation. worthlessness for Black children. Noticeably, DeGruy does not identify religion as a belief or contributor to beliefs that perpetuate trauma. Religion as a vehicle for trauma has been posited by authors such as Sikivu Hutchinson (2011, 2013), Anthony Pinn (2017), and Cristopher Cameron (2019).

Intergenerational Black trauma is very real. It is constantly reference in common terms by members of the Black community. In most cases, Black people talk about it comically. Many Black-centered sitcoms have also taken this approach. Shows like *Everybody Hates Chris* and *Black-ish* try to balance the good and the bad of these intergeneration adaptations; Usually, the good and bad are wrapped in a single scene or joke. However, intergenerational Black trauma is a serious influencer of formations of privacy, justice, and freedom in the Black Household. This theory of generationally inherited behaviors and beliefs is integral for understanding the experiences and perspectives of some of the Black participants in this study.

The specific connection of personal privacy, personal freedom, and personal ownership is passed down generationally from parent to child. This connection manifests as a form of trauma — Noshi does not describe the experiences which taught them privacy as pleasant. However, what Noshi describes is not unique. It fits within the larger array of trauma thought to be passed down from slaves to their descendants that DeGruy and others (Harrisson-Ross 1973; Staples 1993; Boyd-Franklin 1996; Bradley 1996; Raymond et al. 1998) argue argue are both internally reified through childrearing customers and externally reified through modern forms of enslavement and discrimination. The association of privacy, freedom, and ownership are no coincidence in the American context. The inability of slaves to legally own their own bodies and assert ownership of their own bodies justified all necessary methods of policing and surveillance (Finkelman 2012), even building slave quarters within view of the master's house (Joyner 2003; Prunty 1955; Orser and Nekola 1985; Barrow 1881). Because slaves were the legal property of others and denied autonomy, any imagined entitlement to privacy by them conflicted with the master's primary legal obligation to secure and maintain their "goods" (Wahl 1997); they were not allowed agency. Despite the trauma associated with privacy, freedom, and ownership norm acquisition in their upbringing, Noshi perceives of ownership as positive; ownership is a domain through which privacy is extended, and conversely, privacy is a field that protects ownership. For example, Noshi owning his childhood journal may have created an expectation of privacy, yet without the sense that the journal is unviewable or unusable by others, the sense of ownership disappears.

Tean & The Black Religious Household

Tean is a biracial Black woman. She spent many of her formative years living in the suburbs of Chicago and in Southern California. From an early age, she found an outlet in the online space. It offered her access to Japanese music, gothic culture, and a community of people like herself; those who were interested in society at the margins. She grew up as an only child to a devoutly Christian single mother, and the online space gave her independence. Like Noshi, she grew up under the philosophy that ownership, freedom, and privacy were connected; And she didn't have any. Tean's offline world was the Black religious household.

I would like to include religion as one of or contributing to the beliefs that perpetuates trauma because this is what is expressed by some of my participants. Tean was taught to be "quiet, be seen and not heard. Don't speak unless you're spoken to". She ruminates that contemptuousness in the Black household is connected to generational trauma from slavery.

> The more I watched slavery movies as a child, the more I associated it with slavery. I wondered if the way that the slave masters treated their slaves didn't get passed down into Black culture, to where you still talk down to your own children, your own family. You know, 'Don't walk away when I'm speaking to you!'

Although Tean does not explicitly mention privacy, in this case, the parent robs the child of privacy by eliminating their access to any space they may perceive as a safe haven for cherished things and emotions. And more disturbingly, the adult invades the boundaries of emotional expressivity. The personal, the body loses its privacy, and the parent assumes ownership and therefore control of the child.

DeGruy recounts witnessing a similar experience. A Black mother and her children are waiting in line in a bank. There is also a White woman and her children waiting in line. DeGruy notices that the Black mother will not allow her children to explore or act on their own curiosity, in stark contrasts to the white mother. In addition, DeGruy notices that when the Black mother's daughter tries to create privacy, by hiding below the lip of the counter at which her mother talks to the clerk, another Black woman disallows reprieve (6-7).

When it comes to the concept of the Black household and privacy based on ownership, Tean similarly feels similarly to Noshi. In her house, she barely had the opportunity to close her room door, let alone lock it. She connects the lack of privacy to a prominence of misogyny in the Black religious community. The patriarchal hierarchy means that all members of the community outside of the male figureheads have little claim to ownership, freedom, or privacy. In a home with a single mother — who unbridledly denied Tean privacy — any hope of escaping disprivacy was placed in the heavenly patriarch. Unfortunately, the Christian god could not empathetically negotiate for privacy on Tean's behalf despite it being much needed. Instead, god and the Bible were used to justify Tean's oppression: "We are all God's children!" In some cases Tean's mother invaded her privacy for the specific purpose of praying over her "to shield her from the devil". Tean spoke frequently of her fears of being intruded upon by her mother; she would come into her room unannounced to check on her, tell her about the lord. The anxiety from these experiences is with Tean presently.

Seva at the Intersection of Analog and Digital

Seva no longer spends much of her time in the online space. She occasionally posts on instagram — pictures of her smiling and just enjoying life. But other than these brief moments online, she doesn't spend hours on the platform chatting, watching lives streams, or commenting on posts. However, Seva found an escape in the digital world as a teenager. It was her window out of a Black household, like Tean's, led by a single mother.

> My mom was very invasive through my growing up and would always look at my texts, look at my Facebook, go through my messages. It caused a lot of issues that I feel just never needed to arise.

Seva does not reveal what her mother looked for when she perused her phone and social media — Black parents are not usually transparent in their intentions, most likely an inherited behavior. However, she does reveal what she worried that she would find. Seva was gay, and she had not revealed this to her parents. Her mom might find something that would out her. Furthermore, she was hiding a growing interest in goth fashion — a huge no-no in christian Black families.

For Seva ownership, freedom, and privacy were complicated by the fact that she was entrusted with a cellphone that only she used. She was entrusted with a cellphone that had access to realms, social media, that were not reachable simply by unlocking the device. Her mother did not know her Facebook password. This differs from the situations of both Noshi and Tean. Having access to the online environment emboldened Seva; it allowed her to pick and choose her battles.

> I wouldn't want my mom to see me in my goth attire, but I posted anyways. I know she's going to comment on it anyways. That is something where like, I want her to have to see that. I could just keep the photos to myself, but I don't feel like letting her have that much power over what I want to post.

Trauma & Privacy

These participants, who are Black, Brown, and Queer, allude to a pervasive intergenerational Black Trauma that shapes privacy. They speak of this intergenerational trauma in terms of the Black household, which they perceive to be distinctly different than other households. This distinct difference can be both positive and negative — these participants do not deny that their very particular upbringings probably shielded them from violence, drugs, and what many call “white people shit”. However, when these participants speak of privacy, they speak with palpable bitterness. That bitterness is directed towards their “homes”, their “parents”. For them, it's hard to imagine that, in their safest space and with the people who are supposed to nurture and guide them, care and love were expressed through control. However, most of all, they feel there was no sense of justice.

Most Black children have a moment when they pose the question, “Why you do me like that?” And most often, they are met with some variant of, “because, out there, that’s how they going to treat you!” Many Black parents have taken their own experiences, and those of their elders, directly into the home. Many Black adults are made to know “their place” by their white counterparts (). In order to survive in a world where excellence and crudeness are both equally punished, many Blacks must learn to “dance” — an invaluable form of deceit that is one of few ways to survive in a world dominated by whiteness. Parents appear to bring the trauma of “walking the tightrope” to their parenting. They are always on-guard. And they exercise maximum control over their children, leaving little room for privacy. While their intentions may be good, and some would argue are justified, the children are then traumatized by experiences they have never had and quite possibly will never have.

Black participants in this study had a strong association between privacy and justice. I posit that privacy becomes synonymous with justice for these participants. Whether it be by agreement or by a purchasing act, the participants in this section could not secure privacy in childhood, in the Black household.

For these participants explicitly, and for others who only alluded to the Black household, the past trauma endured by their ancestors and the trauma endured by their parents shapes their perceptions of privacy. Instead of privacy being negotiated based on trust and respect or even the necessity of understanding how people negotiate privacy, Black children in the Black household are seemingly taught privacy by the absence of it. They learn that privacy and ownership, specifically accomplished through a purchasing act, are extricably connected. Trust or respect which are usually traded for or factor into the negotiations for privacy are diminished.

The disconnect is shown in the case of Seva. She is entrusted with a cellphone, but privacy does not follow. This leads many Black persons to perceive justice or injustice in relation to privacy through the lens of the distribution of benefit [distributive justice]. Even personal agency born from the body [procedural justice] is detached from privacy, and that legacy seems to extend from slave livelihood. Although some critique the determinism and empiricism of theories like DeGruy's, it is hard to assert that slavery has not had and still does not affect Black life in a major way.

A famous retort used by Black parents during intense situations with their children is "I brought you into this world, I'll take you out of it!". It encapsulates how children in some Black children encounter antiquated ideas about ownership in the Black household. Under these notions of ownership, Black children do not have their own will, desires, or entitlements. I consulted with non-Black friends to ask about this phrase. Some had heard it used by their parents, but they perceived it as more of an idiomatic threat. However, Black friends perceived that there was some deeper meaning. When one's parent speaks these words, they subvert all other ideas of existence. The child listening is not the child of a nation, not the child of society, not the child of god, but the sole possession of the parent.

Patricia Hill Collins challenges what she calls the “property model” of childrearing in Black Feminist Thought (2000) by arguing that communal responsibility for children subverts “capitalist property relations”:

> African-American women who continue community-based child care challenge one fundamental assumption underlying the capitalist system itself: that children are “private property” and can be disposed of as such. Under the property model that accompanies the traditional family ideal, parents may not literally assert that their children are pieces of property, but their parenting may reflect assumptions analogous to those they make in connection with property. For example, the exclusive parental “right” to discipline children as parents see fit, even if discipline borders on abuse, parallels the widespread assumption that property owners may dispose of their property without consulting members of the larger community. By seeing the larger *community* as responsible for children and by giving othermothers and other nonparents “rights” in child rearing, those African-Americans who endorse these values challenge prevailing capitalist property relations. (p. 182)

However, this holds true as long as there is a community for which Black children can participate. The 90s and naughts were tough times for Black neighborhoods. Many Black parents, and in particular Black single mothers, kept their children inside for fear of their safety. This meant that opportunity for community parenting was rare, with the exception being the church. In addition, what Collins identifies as a shared “right” to punish is precisely the problem of intergenerational Black trauma. Why is punishment a shared commodity? If anything, the communal “right” to punish parallels the sentiment towards slaves. Anyone of the power group could capture, beat, and maim the slave for the purpose of reinforcing physical and mental realities of their enslavement. The slave remains the sole property of the owner. The child remains the property of the parent.

For those raised in the Black household, their conceptions of privacy are shaped by their ancestors and parents' trauma. The parents, themselves, are just as much victims as the children. They too are shaped by the vessel of enslavement, religious thought, and the precocity of Black life, their socio-economic status. Undeniably, there may be other factors that contribute to strict privacy measures in Black households, and affluent non-religious Black households can surely lack privacy; however according to this study's Black participants, there is a distinctness to the Black household which informs their constructions of privacy and its relations to justice and in-justice. The institution of the Black household, as identified by these participants, results in a very specific first-time internet user, one that is obsessed with ownership of online space. These users often enter into the online space looking to exercise personal ownership, personal freedom, and personal privacy. Many know that their parents cannot claim ownership of the online space and so they enter the online space with the purpose of expressing their genuine selves.

CHAPTER VI: DIFFERENT, YET THE SAME: GENERATIONAL DIFFERENCES

Although all users of color interact with the white space, whether they respond to it depends on their perceptions of privacy, their sense of justice, and their level of empowerment. When examining the interviews of this study's participants, I noticed a trend; those who were Millennials, or older, tended to be very concerned about justice in the online space, and those who were Generation Z did not express much concern. This chapter explores how participants perceptions of privacy effects their digital privacy strategies. I argue that how participants think of privacy affects the privacy strategies they employ as well as the rationalizations they use to justify their practices. Interestingly, all participants expressed some understanding of privacy in the online space, but all did not express a right to privacy in the online space. This study assumes that a disbelief in privacy precludes feelings of unjust or just monitoring in the online space. Furthermore, the extent of the perception of a right to privacy affects what forms of justice are conceived by participants when presented with what I call a *disprivacy event*: an event in which the participant has been asked to abdicate a degree of their privacy or an event in which the participant's privacy has been usurped. Two groups emerge when examining direct statements on privacy along with comments on terms of service agreements: Millenials and Generation X versus Generation Z.

A Right to Privacy

Many older Back participants (Millennials and older) construct their sense of privacy from their understanding of the online space as one that is structured and hierarchical. This may stem from their upbringing, such as in a Black household, however many of the participants and others who I engaged with in conversation about my research who were not Black expressed a similar form of trauma.) From the perspective of these older Black participants, people in the online space have rights; there are laws and rules; and there are adjudicators (institutions, groups, and individuals), just as in the offline world. Millennials and older generations understand that the systems of the online space are just as imperfect and malleable as those in the offline space. This assumption of imperfection allows them to perceive instances of justice and injustice in the online space. They do not take a platform's word on anything. I asked Ery what was the first thing that comes to mind when they hear digital privacy, and they responded, "Like, all the ways that [it] can be violated or ways that our online activity is being monitored without our direct knowledge. And Facebook definitely comes to mind."

In just two sentences, Ery reveals that they believe there is such a thing as privacy in the online space, expresses notions of justice and injustice in relation to privacy, and identifies the perpetrators of disprivacy. Ery believes there is a right to privacy in the online space but expresses that it is precarious and endangered by the machinations of the space's ruling institutions. Ery also alludes to a conceptualization of justice when it comes to privacy that relies on notice or communication of action; this is recognizably procedural justice. Injustice in the online space is not equated simply with being monitored from Ery's perspective; instead, being monitored without due consultation and notification is unjust.

Hione similarly cites infractions to digital privacy as her first thought when asked directly about digital privacy. Later in our discussion when discussing the dissemination of school computers for at home student use, Hione asserts a right to not be monitored: "If you're using a personal computer, then [the school] shouldn't have a right to monitor you." In this case, Hione determines the justness of schools monitoring students (and possibly parents) on laptops at home via a material wellness framework. She rationalizes that since the users of a school provided laptop receive some benefit, they potentially cede the right to privacy. However, in the case of using a personal laptop (to complete the schoolwork), the invasion of privacy would be unacceptable; there is no proportional benefit to the students.

Ayan is a Japanese immigrant who has lived most of his life in the U.S. Although he accepts the pronoun "he", Ayan identifies as non-binary. He is passionate about activism and is a tireless educator who focuses on helping his students think critically. He is at the tail end of Generation X and barely has an online presence. However, this was not always the case. Ayan used to use all of the major social media platforms, but he states that his experiences online and offline have contributed to his self-deplatforming. In a impassioned conversation about terms of service agreements, Ayan passionately talked at length about his perception of the online space, whether people have a right to privacy, and how people's right to privacy is being stripped away.

> I think it's intentionally cumbersome for us to figure all this out. It's always changing. Our user agreements are always changing. The things in the fine print, you know, our rights, consumer rights, user rights, etc. It's constantly changing. And it's not just in physical fine print, but it's also in big words, which, you know, attorneys, corporate attorneys, IP attorneys are intentionally wording things a certain way so they have a margin of rights or a margin of power that they can operate in.

Later in the interview, Ayan goes on to connect the problems of the online space to larger problems with governance in the American system. He perceives injustice in the online space as supporting "real world" injustice and vice-versa. He vehemently believes that people have a right to privacy in the online space, but he is soberingly aware that every day it is becoming more difficult to operationalize, let alone conceptualize, privacy while being online. He believes procedural justice is effervescent unless were act quickly.

Leone is a Black man born and raised on the South Side of Chicago. Like many there, he has a strong drive to leave his mark on the world. He is a millennial, but he is already a school principal. He participated in the study with some trepidation. He had many questions. He says "I like to do my homework!" He uses many of the major social media platforms and phone apps.

When asked about digital privacy, he is more hesitant than other participants to admit that it exists. Eventually in our conversation, he started to speak of privacy in the online space, and he even alluded to his belief in a right to privacy. The conversation vacillated between major breaches committed by hackers and social media platforms sharing data with the government. When asked which he was more concerned about, the government or hackers, Leone told me:

> I'm equally worried about either one of them. I think that what I worry about with a hacker is that they can easily distribute your information and more or less ruin your life, anything that you have on your digital platform that your trying to keep private. You know, and in our society, you're guilty until you prove yourself innocent. What I worry about with the government is that the government encroaching and having broad sweeping powers to do whatever they want to with your data, your metadata. I just feel like it's an encroachment on privacy, and I also think that it will lead to a slippery slope where it becomes big brother-ish.

By stating that the government would be encroaching upon an individual's privacy, Leone reveals that he does believe there is an individual right to some form of privacy in the online space; though, the extent of that privacy is not something that Leone has decided.

Millennials believe that privacy in the online space exists, there is a right to privacy for all users, there are systems that assign and manage online privacy — which both intersect and are undefended from larger structures in society, and violating the right to privacy is unjust. They feel that individuals have power in the online space, although this is fleeting. And they do not understand the internet to be an innate institution; It has a history and a trajectory. There is a possibility that the online space could look completely different than it does now in the future.

A Right or a Rite?

Younger participants, who mostly align with the increasingly used Generation Z and Zoomer generational name, conceive of online disprivacy as a rite of passage that leads to social and economic benefit. They have concerns about privacy, but the younger participants from this generation generally do not understand the problem of privacy in terms of procedural justice like older participants. Instead, they examine the online environment with a sense of concern about distributive justice; they are concerned that they get something of value in turn for disprivacy, and most of them are currently content with the tradeoff. Through this study I have found that younger participants believe there is an equitable tradeoff with platforms for their disprivacy, the focus of their concerns about online safety is other persons in the online space.

Cosan is a current undergraduate student and is one of the younger participants in the study. He spends a great deal of his free time in the online space. He uses major platforms such as Facebook, Twitter, and TikTok daily. When asked about privacy in the online space, he challenged that there is such a thing. Cosan studies cybersecurity, and from his perspective, the major platforms already know what they are interested in knowing about the majority of people. He expressed that he was fine with this situation; although, he wished it could be different. Cosan says that he feels the constant surveillance by platforms is a benefit to him. Instead of seeing ads for products that he has no interest in, he gets ads only for things he actually cares about. The same goes for news stories and alerts. And because the platforms know him well, Cosan feels that they can introduce him to new things that he would not have discovered on his own.

However, when the topic turns to other people in the online space Cosan feels very differently. Cosan speaks emphatically of his experience being harassed by a white female coworker. She first found him on LinkedIn where he felt comfortable being connected to her; he felt in control. However, soon she began finding all of his social media accounts, even those that had no easy association to him. Cosan said this made him worry.

> She would share personal information of other employees very personal information to me or other employees, which I do not consider as ok. Because it's not for her to share that information. It's not her choice. Now, I feel bad for the person that trusted her with that information, And I would not share my personal information with her. Thats the reason why I did not accept her invite on my [other] social media. Because I never know what could be used against me.

In a subsequent conversation, Cosan talked at length about the precariousness of being a minority. A major contributor to his anxiety about his coworker stalking his "private social media" (Cosan uses this to differentiate with what he considers public social media, such as LinkedIn) was the power differences between different racial groups.

Roi recently graduated from a four year university. He frames the benefits of disprivacy at the societal level. People who are in accidents can be located easily, traffic can be routed around accidents, data can be used to track pandemics. However, he admits that he stopped playing Pokemon Go because of his concern at developers hiding surveillance measures in the app options. He feels uncomfortable with all of the things in the terms of service that he agrees with, but he still has social media accounts. He sites social reasons, but also emphasizes the potential career benefits of digital participation.

> To be honest, I don't really like deplatform myself, I try not to put up anything that I would ever feel like I needed to take down. I try to think that out ahead of time and actually use it to my advantage. Having no online presence actually does play to your disadvantage, especially in the modern world. So unfortunately, you know, we we have to think about how we craft an image of ourselves. And, you know, it's actually helped me lead to jobs. It's, it's been wonderful. But I have to be, you know, thoughtful about how I do that. I can't be like putting up there, you know, hey, I totally just got blasted this weekend. I'm so drunk right now and sending pictures, you know, flashing the White House or something. I don't know. But you know, at the same time, I put out there productive things that I am doing within my own work fields and really help strengthen the identity for myself and build up consumer confidence in a way. So I've never come off of a platform.

While Roi finds the actions of major platforms to be suspicious, manipulative, and invasive, he does not leave these platforms. Instead, he believes that he can navigate them effectively by cultivating the “right” online image. He does this because, as he says, he has achieved career benefits from the online space. This shows that he is mainly concerned about distributive justice in the online environment. He cares about how much benefit he reaps versus the trade off in dis-privacy. While he expresses concern at major platforms information gathering practices, his privacy concerns revolve around managing and maintaining interpersonal relationships. With one exception, he did admit to deleting the Pokemon Go app because of concerns of being listened to and watched covertly.

Jody is a current undergraduate student at a pricey private four-year university. This contrasts their humble upbringing on the South Side of Chicago as a young Latino. He grew up in Little Village, and, as they say, he feels proud of his neighborhood, his people, and thimself. He has already made a huge impact in their community via their volunteering and leadership. As an avid debater, Jody is used to reading and processing many pages of information for the purpose of taking a position to argue; though this is what he said about terms of service agreements.

> I guess we're so attracted to what platforms bring, that we don't care about what those repercussions are. Because they way that these platforms are promoted, and it's like they're so big and shiny and bright and so attractive that everyone just wants to be on them. Do you honestly think people are going to take the time to read [the terms of service]?

Jody brazenly admits that he does not read the terms of service agreements for social media platforms. He also alludes that joining social media for him was about following and finding community. In other words, he eschews access to procedural justice for potential distributive justice. For him the benefit is social. He does feel that platforms should be more transparent in the rights they steal from their customers, and he agrees with increasing discussions that terms of service agreements be simplified to increase readability for the average user.

Younger participants in this study conceive of privacy in the online environment very differently than their millennial counterparts. They are not as concerned with institutions compromising their privacy; instead, they are more concerned about other individuals in the online space. They believe that individuals are more likely to have a negative impact on their digital privacy. When it comes to major platforms, they are more concerned with distributive justice. They want to know that there is some explicit proportional benefit to having their privacy invaded by the major platforms. Younger participants seem more concerned with filtering their online presence because of their wariness of other people, but they are less likely to actually leave platforms or challenge their practices because they are scared of compromising the social and economic benefits they believe they will reap. The way that younger participants in this study think about the online space and digital privacy is like a rite of passage. They believe that disprivacy because of the practices of major platforms is unavoidable. They believe that there is a correct way to navigate the online space that requires sacrifice, but at some point there will be a return on the sacrifice.

Two Houses

When looking at the privacy strategies employed by the seventeen study participants, there is a trend for older participants; they block [contact management], curate their posts [access setting], and some eventually self-deplatform [privacy setting] if the two previous strategies do not work to secure them digital privacy — eight participants in this study revealed that they hey self-deplatformed; they were all millennial or older participants. Younger participants, Generation Z, very meticulously curate certain content [access setting]. The participants in my study who were younger did not block much [contact management] and none self-deplatformed [privacy setting] from a major social media platform. None of the seventeen formal participants in this study, or others who were informally interviewed, revealed that purposeful aliasing [identity masking] was part of their privacy repertoire.

CHAPTER VII: CONCLUSION

Millennials and Generation Z participants in this study think of the online space in very different ways. Millennials come to the online space with specific intergenerational knowledge that shapes their perceptions of justice and choice of privacy strategies in the online space. Generations Z participants did not seem to have or apply said knowledge when understanding the online space and choosing privacy strategies. Millennials found safety in the online space by self-deplatforming from major social media platforms while Generation Z denied self-deplatforming as a valid method of attaining safety. Instead, they focused on fostering very specific online identities through content curation. Regardless, the collective experiences of this study's participants point to the reality for many people of color in the online space; they do not feel safe.

These feelings point to a more fundamental divide in the online space that has largely been minimized by theorists of the digital divide. Race is still a problem in the online space and functions to empower and disempower certain people online. More often than not, people of color are disempowered. Theorists of the internet and the digital divide ignore or are unable to see this because most of the research is quantitative. The results of this qualitative study support the critical criticism of digital divide research and theorizing by Greene (2016), Selwyn (2004), Stevenson (2009), and Wacquant (2009); theorists of the digital divide have minimized the fundamental issues of the online space with respect to race. Instead, they constantly reify the divide as a technology and knowledge problem because they are ingrained within neoliberal investment interests which are preference delivering cheap labor to the marketplace. The participants experiences shared in this study reinforce the necessity to approach the digital divide in a way that is human-centered and not laden with corporate interests.

In addition to exploring the informal ways in which the digital privacy strategies of the people of color who participated in this study were formed, I asked about formal education related to digital privacy. I asked participants if their education had helped them to understand the online environment and how to find safety within it. Almost all of the participants revealed that they did not receive any guidance from their educational institution. Some revealed that they learned about how to navigate the online space from their parents, others recognized that their privacy behaviors, and those of others, are potentially influenced by norm entrepreneurs in the online space — youtubers, streamers, influencers. This suggests that some are learning about digital privacy and how to think about the online space from the very entities which have an incentive in normalizing easily exploitable behaviors. For Millenials, intergenerational adaptations passed down from their parents through child rearing and storytelling becomes vital in helping them to navigate the online space. For Generation Z, despite equally desiring this information, they do not have it. Integrating the history of the internet and basic internet privacy techniques into coursework would go a long way to helping those who most need and desire this information. And even though white people are not the primary focus of this specific research, they stand to benefit from learning about the history of oppression in the online space as well. So, those who are interested in fighting for justice, equality, and equity do not inadvertently commit the same offense as the streamer for the Zack and Matt show.

The experiences presented in this study provide a glimpse of the glaring trajectory from intergeneration Black trauma to online behaviors by people of color. Though the participants clearly experienced and continue to experience hurt, the picture is not black and white. The trauma they experienced manifests as a potential advantage in the digital space. For this reason, I refer to intergenerational trauma when focusing on the personal experiences, and I use other terms when theorizing on the effect on digital safety.

People of color are leaving the online space, and when they remain they are transient and nomadic. They cannot currently find privacy: online safety. Of this, Morales et al (2016) says "digital participation hinges on social political interpretation" of the online space (111). Whether one participates and how one participates in the online environment is based on how they perceive its existence. For many of the older people of color participants in this study, the online space increasingly supports regimes of oppression. Although we are in the in-between where as a tool the internet is still invaluable to social justice movements, self-expression, and self-actualization, many older participants (Millennials and older) wonder how long we have before we are the ones being moved, told what to express, and told what we are by social media — if we are not already. For many, these fears have driven them to leave major social media platforms and increasingly resign from major social media platforms. The understanding of the online space is very different for Generation Z. They see the online space with the gaze of possibility. This study suggests this may be because of a lack of recognition of the tools of oppression. Perhaps, this is because many younger participants do not carry the intergenerational trauma of older participants — for what reason that may be is outside the scope of this study. Perhaps, their inability to see oppression in the online space is linked to an erasure of the history of the internet, the history of minorities and the internet, the history of Black people and the internet, the history of Black people, Period! A single participants, Anha, said that she received applicable guidance on navigating the online space in her education. The rest were either educated by their intergenerational trauma, which both protects and weighs on them, or they received nothing at all. Without the history of the internet and its use as a tool of oppression, which involves all of us and belongs to all of us, younger participants who increasingly constitute the online space are yielding leverage to the oppressors. In a “deal with a devil”, they trade privacy for benefits they may never reap. This is because the very commodities they seek to exploit, their Blackness, their exoticness, their disprivacy, endangers them. And for those who can endure, the return on disprivacy in the online space is increasingly small.

REFERENCES

Alford, Aaron. “FerociouslySteph is actually right about voice chat being problematic.” *Qrank*, June 16, 2020. https://qrank.gg/more/general/ferociouslysteph-is-actually-right-about-problematic-voice-chat/

Amir, Eli, Shai Levi, and Tsafrir Livine. “Do forms underreport information on cyber-attacks? Evidence from capital markets.” *Review of Accounting Studies* 23, no. 3 (2018): 1177-1206. New York: Springer Publishing. DOI:10.1007/s11142-018-9452-4

Anderson, Elijah. “The White Space.” Sociology of Race and Ethnicity 1, no. 1 (2015): 10-21. DOI:10.1177/2332649214561306

Ashworth, Laurence and Clinton Free. “Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers’ Online Privacy Concerns.” *Journal of Business Ethics* 67 (2006): 107-123.

Bakht, Shayma. “Hate-Hacking and Zoom’bombing’: Racism in the Virtual Space.” *Aljazeera*, June 23, 2020. https://www.aljazeera.com/features/2020/6/23/hate-hacking-and-zoom-bombing-racism-in-the-virtual-workspace

Barrow, David. “A Georgia Plantation.” *Scribner’s Monthly* 21, no. 5 (March 1881): 830-836.

Bing, Jon. “Building Cyberspace: a brief history of Internet.” In Internet Governance: Infrastructure and Institutions, ed. Jon Bing and Lee Bygrave, 8-47. Oxford: Oxford university Press, 2009.

Bond, Shannon “A Must for Millions, Zoom Has a Dark Side - And An FBI Warning.” *NPR*, April 3, 2020. https://www.npr.org/2020/04/03/826129520/a-must-for-millions-zoom-has-a-dark-side-and-an-fbi-warning

Booth, Ken. “Security and Emancipation.” *Review of International Studie*s 17, no. 4 (1991): 313-326. United Kingdom: Cambridge University Press.

Boyd-Franklin, N. *Black families in therapy: a multi systems approach*. New York: Guilford, 1989.

Bradley, C. “Child rearing in African American families: A study of the disciplinary practices of African American parents.” *Journal of Multicultural Counseling and Development* 26, no. 4: 273-281. https://doi.org/10.1002/j.2161-1912.1998.tb00204.x

Buckley, Thomas. *American Foreign and National Security Policies, 1914-1945*, 1st ed. Knoxville: University of Tennessee Press, 1987.

Buzan, Barry. *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, 2nd ed. London: Harvester Wheatsheaf, 1993.

Cameron, Christopher. *Black Freethinkers: A History of African American Secularism (Critical Insurgencies)*. Evanston, Illinois: Northwestern University Press, 2019.

Castells, Manuel. *The Rise of the Network Society, The Information Age: Economy, Society and Culture Vol. I*. Cambridge, Massachusetts: Blackwell, 1996.

———. *The Power of Identity, The Information Age: Economy, Society and Culture Vol. II*. Cambridge, Massachusetts: Blackwell, 1997.

———. *End of Millennium, The Information Age: Economy, Society and Culture Vol. III*. Cambridge, Massachusetts: Blackwell, 1998.

———. *The Network Society: A Cross-Cultural Perspective*. Northampton, Massachusetts: Edward Elgar Publishing, 2004.

Castro, Alex. “Playing Red Dead Online As A Black Character Means Enduring Racist Garbage.” *The Verge*, January 15, 2019. https://www.theverge.com/2019/1/15/18183843/red-dead-online-black-character-racism

Chen, Hongliang, Christopher E. Beaudoin, and Traci Hong. "Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors." *Journalism & Mass Communication Quarterly* 93, no. 2 (2016): 409-429.

Churchill, Ward and Jim Vander Wall. *The COINTELPRO Papers: Documents from the FBI’s Secret Wars Against Domestic Dissent*. Boston, Massachusetts: South End Press, 1990.

Colaressi, Michael. 2020. “How our misunderstanding of the digital and computing revolutions puts democracy at risk (and what to do about it).” *Critical Quarterly* 62, no. 1: 70-80.

Collins, Patricia. *Black Feminist Thought : Knowledge, Consciousness, and the Politics of Empowerment*. Boston: Unwin Hyman, 1990.

Cowley, Stacey and Nicole Perlroth. 2019. “Capital One Breach Shows a Bank Hacker Needs Just One Gap to Wreak Havoc.” *The New York Times,* July 30, 2019. (Accessed January 31, 2020). https://www.nytimes.com/2019/07/30/business/bank-hacks-capital-one.html

Davidson, Thomas, Bhattacharya, Debasmita, and Ingmar Weber. “Racial Bias in Hate Speech and Abusive Language Detection Datasets.” Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Italy, August 2, 2019.

DeGruy, Joy. *Post Traumatic Slave Syndrome: America’s Legacy of Enduring Injury and Healing.* Milwaukee, Oregon: Uptone Press, 2005.

Denning, Peter, Hearn, Anthony and William Kern. “History and Overview of CSNET.” *Department of Computer Science Technical Reports*. Paper 348 (1981). https://docs.lib.purdue.edu/cstech/348

Department of State Bureau of Politico-Military Affairs, Final rule. “Amendments to the International Traffic in Arms Regulations, Public Notice 1832” Federal Register 58, no. 139 (July 22, 1993): 39280. https://www.govinfo.gov/content/pkg/FR-1993-07-22/pdf/FR-1993-07-22.pdf

DiMaggio, Paul and Eszter Hargittai. 2001. “From the ‘Digital Divide’ to ‘Digital Inequality’: Studying Internet Use as Penetration Increases.” *Working Paper Series* 15, Center for Arts and Cultural Policy Studies, Princeton, New Jersey.

Dobransky, Kerry and Eszter Hargittai. “The disability divide in Internet Access and Use.” *Information, Communication, & Society* 9, no. 3 (2006): 313-334. DOI:10.1080/13691180600751298

Falling Through the Net: Defining the Digital Divide, July 1999, National Telecommunications and Information Administration. https://www.ntia.doc.gov/report/1999/falling-through-net-defining-digital-divide

Farzan, Antonia. “Memphis Police Used Face Facebook Account to Monitor Black Lives Matters, Trial Reveals.” *The Washington Post*, August 23, 2018. https://www.washingtonpost.com/news/morning-mix/wp/2018/08/23/memphis-police-used-fake-facebook-account-to-monitor-black-lives-matter-trial-reveals/

Finkelman, Paul. “Slavery in the United States: Persons or Property?” In *The Legal Understanding of Slavery: From the Historical to the Contemporary*, edited by Jean Allain, 105-134. Oxford: Oxford University Press, 2012.

Flaherty, Colleen. “White Lies: Prominent scholar outs herself as white just as she faced exposure for presenting herself as Black.” *Inside Higher ED*, September 4, 2020. https://www.insidehighered.com/news/2020/09/04/prominent-scholar-outs-herself-white-just-she-faced-exposure-claiming-be-black

Foley, Paul. “Does the Internet Help to Overcome Social Exclusion.” *Electronic Journal of e-Government* 2, no. 2 (2004): 139-146.

Fuchs, Christian and Eva Horak. “Africa and the Digital Divide.” *Telematics and Informatics* 25 (2008): 99-116.

Fuller, Christopher. “The Roots of the United States’ Cyber (In)Security.” *Diplomatic History* 43, no. 1(2019): 157-185. Oxford: Oxford University Press. DOI:10.1093/dh/dhy038

Gervais, Joe. Privacy vs. Security. norton.com. https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html

Goedhart, Nicole, Breorse, Jacqueline, Kattouw, Rolinka, and Christine Dedding. “‘Just Having a Computer Doesn’t Make Sense’: The Digital Divide from the Perspective of Mothers with a Low Socio-Economic Position.” *New Media & Society* 21, no. 11-12 (2019): 2347-2365. DOI:10.1177/1461444819846059

Greene, Daniel. “Discovering the Divide: Technology and Poverty in the New Economy.” *International Journal of Communication* 10 (2016): 1212-1231. https://ijoc.org/index.php/ijoc/article/view/3969/1587

Guynn, Jessica. “Facebook and Instagram to Study Racial Bia Against African Americans, Hispanics on Their Platforms.” *USAToday*, July 22, 2020. https://techxplore.com/news/2020-07-facebook-instagram-racial-bias-african.html

Hand, Patrick, “Probable Cause Based on Inaccurate Computer Information: Taking Judicial Notice of NCIC Operating Policies and Procedures,” *Fordham Urban Law Journal* 10, no. 3 (1982): 497-510. https://ir.lawnet.fordham.edu/ulj/vol10/iss3/5

Hansen, Mary. “Illinois Looks to Map Who Has Internet Access and Who Doesn’t.” *NPR Illinois*, Jan 2, 2020. https://www.nprillinois.org/post/illinois-looks-map-who-has-internet-access-and-who-doesn-t#stream/0

Harrison-Ross, Phyllis. *The Black Child: A Parent’s Guide to Raising Happy and Healthy Children*. New York: Berkeley Publishing Company, 1973.

Hemphill, Stuart R. “Protection of Privacy of Computerized Records in the National Crime Information Center.” University of Michigan Journal of Law Reform 7 (1974): 594-614. https://repository.law.umich.edu/mjlr/vol7/iss3/9

Hilbert, Martin. “Digital Gender Divide or Technologically Empowered Women in Developing Countries? A Typical Case of Lies, Damned Lies, and Statistics.” *Women’s Studies International Forum* 34, no. 6 (2011): 479-489. DOI:10.1016/j.wsif.2011.07.001

Hoerl, Kristen and Erin Ortiz. “Organizational Secrecy and the FBI’s COINTELPRO-Black Nationalist Hate Groups Program, 1967-1971.” *Management Communication Quarterly* 29, no. 4 (2015): 590-615. DOI:10.1177/0893318915597302

Hutchinson, Sikivu. *Godless Americana: Race and Religious Rebels*. Infidel Books, 2013.

———. *Moral Combat: Black Athiests, Gender Politics, and the Values Wars*. Infidel Books, 2011.

Jackson, Lauren. “The Layered Deceptions of Jessica Krug, The Black-Syudies Professor Who Hid That She Is White.” *The New Yorker*, September 12, 2020. https://www.newyorker.com/culture/cultural-comment/the-layered-deceptions-of-jessica-krug-the-black-studies-professor-who-hid-that-she-is-white

Jackson, Lauren. “The Women ‘Blackfishing’ on Instagram Aren’t Exactly Trying to Be Black: They’re Engaging in Something More Insidious.” *slate.com*, November 29, 2018. https://slate.com/culture/2018/11/blackfishing-instagram-models-emma-hallberg-appropriation.html

Jaeger, Birgit. “Trapped in the Digital Divide? Old People in the Information Society.” *Science & Technology Studies* 17, no. 2 (2004): 5-22.

Johnson, David. 2006. *The Lavender Scare: The Cold War Persecution of Gays and Lesbians in the Federal Government*. Chicago: University of Chicago Press.

Joyner, Stefanie. “Slave Housing Patterns within the Plantation Landscape of Coastal Georgia.” Unpublished Master’s thesis, University of Florida, 2003. https://ufdc.ufl.edu/UFE0000714/00001

Kafer, Gary. “Big Data Biopolitics: Computing Racialised Assemblages in Terrorist Watchlist Matching.” *Digital Culture and Society* 5, no. 1 (2019): 23-42. DOI:10.14361/dcs-2019-0103

Kahn, Robert. Demonstration at International Computer Communications Conference. RFC 371. July 12, 1972.

———. Resource Sharing Computer Communication Networks. *Bolt Beranek and Newman Report* No. 2459. July 31, 2971.

Kanengo, Diallo. “Black trauma porn, slacktivism, and chicken soup for the activist soul.” *cherwell.org*, June 15, 2020. https://cherwell.org/2020/06/15/black-trauma-porn-slacktivism-and-chicken-soup-for-the-activist-soul/

Kania-Lundholm, Magdalena. “Slow Side of the Divide? Older ICT Non- and Seldom-Users Discussing Social Acceleration and Social Change.” *Digital Culture and Society* 5, no. 1 (2019): 85-103. DOI:10.14361/dcs-2019-0106

Krauss, Rebecca. “Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants.” Paper presented at the Joint Statistical Meetings, Miami Beach, FL, August 1, 2011.

Lederberg, Joshua. “Digital Communications and the Conduct of Science: The New Literacy.” *Proceedings of the IEEE* 66, no. 11 (1978): 1314-1319.

Levine, Jon. “Rachel Dolezal, who posed as black, ‘vindicated’ by Black Lives Matter movement.” *New York Post*, July 4, 2020. https://nypost.com/2020/07/04/rachel-dolezal-vindicated-by-black-lives-matter-movement/

Levy, Marc. “Is the Environment a National Security Issue?” *International Security* 20, no. 2 (1995): 35-65.

Licklider, J.C.R. *Libraries of the Future*. Cambridge, Massachusetts: MIT Press, 1965.

Licklider, J.C.R. and Robert Taylor. “The Computer as a Communication Device.” *Science and Technology Magazine*, April 1968.

Licklider, J.C.R. and Albert Vezza, “Applications of Information networks,” *Proceedings of the IEEE* 66, no. 11 (1978): 1330-1346.

Liff, Sonia and Adrian Shepherd. “An Evolving Gender Digital Divide?” Oxford Internet Institute, *Internet Issue Brief* No. 2, July 2004.

Loedenthal, Michael. “When cops ‘go native’: policing revolution through sexual infiltration and panopticonism.” *Critical Studies on Terrorism* 7, no. 1 (2014): 24-42. http://dx.doi.org/10.1080/17539153.2013.877670

Lukasik, Stephen. “Why the Arpanet Was Built.” *IEEE Annals of the History of Computing* 33, no. 3 (2011): 4-21. IEEE Computer Society DOI:10.1109/MAHC.2010.11

McNamara, Chan Tov. “White Caller Crime: Racialized Police Communication and Existing While Black.” *Michigan Journal of Race and Law* 24, no. 2 (2019): 334-415. https://repository.law.umich.edu/mjrl/vol24/iss2/5

Mehra, Bharat, Merkel, Cecelia, and Ann Bishop. “The Internet for Empowerment of Minority and Marginalized Users.” *New Media & Society* 6, no. 6 (2004): 781-802. DOI:10.1177/146144804047513

Miller, Ben, Jennifer Olive, Cameron Kunzelman, Kelly Bergstrom, Wessel Stoop, Susan Benesch, Cindy Berger, et al. “Notoriously Toxic: Understanding the Language and Cost of Hate and Harassment Online Games.” Georgia State University Research Foundation, Inc., Atlanta, Georgia.

Morales, José, Antino, Mirko, De Marco, Stefano, and Josep Lobera. “The New Frontier of Digital Inequality: The Participation Divide.” *Revista Española de Investigaciones Sociológicas* 156 (2016): 97-116. DOI:10.5477/cis/reis.156.97

Moussa, Mohamed and Joanna Seraphim. “Digital Gender Divides and E-Empowerment in the UAE: A Critical Perspective.” *International Journal of Education and Development Using Information and Communication Technology* 13, no. 3 (2017): 145-161.

Njølstad, Olav. “Atomic Intelligence during the Cold War,” *Journal of Strategic Studies* 29, no. 4 (2007):653-673. London: Routledge. DOI:10.1080/01402390600766114

O’Neil, Dara and Paul Baker. “The Role of Institutional Motivations in Technological Adoption: Implementation of Dekalb County’s Family Technology Resource Centers.” *The Information Society* 19 (2003): 305-314. London: Taylor & Francis. DOI: 10.1080/01972240390227886

Orser, Charles and Annette Nekola. “Plantation Settlement from Slavery to Tenancy: An Example from a Piedmont Plantation in South Carolina.” In *The Archaeology of Slavery and Plantation Life*, edited by Theresa A. Singleton. Orlando: Academic Press, 1985.

Packard, Noel. “Three Kinds of Demand Pull for the ARPANET Into the Internet.” *Cogent Social Sciences* 6, no. 1 (2020): 1720565. DOI:10.1080/23311886.2020.1720565

Padilla, Mariel. “Black Deliveryman Says He Was Blocked and Interrogated by White Drive.” *New York Times*, May 17, 2020. https://www.nytimes.com/2020/05/17/us/black-delivery-driver-okc-travis-miller.html

Payton, Fay Cobb. “Rethinking the Digital Divide.” *Communications of the ACM* 46, no. 6 (2003): 89-91.

Pettit, Harry. “Sick Hack: Sick gamers use cheats to spawn KKK characters that chase and kill black players in Red Dead Redemption.” *The Sun*, June 17, 2020. https://www.thesun.-co.uk/tech/11887407/red-dead-redemption-2-cheats-kkk-black-players/

Piko, Bettina. “Gender Differences and Similarities in Adolescents’ Ways of Coping.” *The Psychological Record* 51 (2001): 223-235. DOI:10.1007/BF03395396

Pinn, Anthony. *When Colorblindness Isn’t the Answer: Humanism and the Challenge of Race (Humanism in Practice)*. Durham, North Caroline: Pitchstone Publishing, 2017.

Prunty, Merle. “The Renaissance of the Southern Plantation.” *Geographical Review* 45, no. 4 (October 1955): 459-491. DOI:10.2307/211613

Pyle, Christopher. “Military Surveillance of Civilian Politics, 1967-1970.” PhD diss. Columbia University, 1974.

Raymond, Henry, Jones, Fred, and Vanessa Cooke. “African American Scholars and Parents Cannot Blame Current Harsh Physical Punishment of Black Males on Slavery: A Response to ‘Cultural Interpretations of Child Discipline: Voices of African American Scholars’.” *The Family Journal: Counseling and Therapy For Couples and Families* 6, no. 4 (October 1998): 279-286.

Reisdorf, Bianca and R.V. Rikard. “Digital Rehabilitation: A Model of Reentry Into the Digital Age.” *American Behavioral Science* 62, no. 9 (2018): 1273-1290.

Ritzhaupt, Albert, Liu, Feng, Dawson, Kara and Ann Barron. “Differences in Student Information and Communication Technology Based on Socio-Economic Status, Ethnicity, and Gender: Evidence of a Digital Divide in Florida Schools.” *Journal of Research on Technology in Education* 45, no. 4 (2017): 291-307.

Rogers, Everett. “The Digital Divide.” *Convergence: The International Journal of Research into New Media Technologies* 7, no. 4 (2001): 96-111. Newbury Park, California: Sage Publications. DOI:10.1177/135485650100700406

Rogers, Juan. “Internetworking and the Politics of Science: NSFNET in Internet History,” *The Information Society* 14 (1998): 213-228.

Schradie, Jen. “The Digital Production Gap: The Digital Divide and Web 2.0 Collide.” *Poetics* 39 (2011): 145-168. DOI:10.1016/j.poetic.2011.02.003

Selwyn, Neil, Gorard, Stephen and Sara Williams. “Digital Divide or Digital Opportunity? The Role of Technology in Overcoming Social Exclusion in U.S. Education.” *Education Policy* 15, no. 2 (2001): 258-277. Thousand Oaks, California: Corwyn Press.

Selwyn, Neil. “Reconsidering political and popular understanding of the digital divide.” *New Media & Society* 6, no. 3 (2014): 341-362. DOI:10.1177/1461444804042519

Sholars, Mike. “Gamers Like PewDiePie Are Why I Don’t Play Online.” *Polygon*, September 21, 2017. https://www.polygon.com/2017/9/21/16341458/pewdiepie-racial-slurs-online-gaming

Solomon, K. “Disability divide,” *The Industry Standard*, 3 July, 2000. Online.

Saint Félix, Doreen. “‘The Rachel Divide’: Review: A Distubing Portrait of Dolezal’s Racials Fraudulence.” *The New Yorker*, April 26, 2018. https://www.newyorker.com/culture/culture-desk/the-rachel-divide-review-a-disturbing-portrait-of-dolezals-racial-fraudulence

Sap, Maarten, Gabriel, Saadia, Choi, Yejin, Smith, Noah, and Dallas Card. “The Risk of Racial Bias in Hate Speech Detection.” Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Italy, August 2, 2019, 1668-1678.

Staples, R. *Black Families at the Cross Roads: Challenges and prospects.* San Francisco: Jessey-Bass, 1993.

Stephan, Bijian. "Get Up, Stand Up." *Wired Magazine Special Issue*, October 2015. https://www.wired.com/2015/10/how-black-lives-matter-uses-social-media-to-fight-the-power/

Steve, Katelyn. "*Victory, a Loss, or a Draw?*: Assessing the efficacy of the FBI's COINTELPRO methods against the Black Panther Party in Chicago." *Journal of Military and Strategic Studies* 18, no. 4 (2018): 73-109.

Stevenson, Siobhan. "Digital Divide: A Discursive Away from the Real Inequities." *The Information Society* 25, no. 1 (2009): 1-22. DOI: 10.1080/01972240802587539

Taglang, Kevin. 2020. "Illinois Addresses the Digital Divide." *Benton Institute for Broadband & Society Weekly Digest*, August 14, 2020. https://www.benton.org/blog/illinois-addresses-digital-divide

Talesh, Shauhin. "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses." *Law & Social Inquiry* 43, no. 2 (2017):417-440. United Kingdom: Cambridge University Press.

Taylor, Flint. "The Torture Machine: Racism and Police Violence in Chicago." *DePaul Journal for Social Science* 12, no. 1 (Winter 2019): 1-7. https://via.library.depaul.edu/jsj/vol13/iss1/7

"Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and Under Water." Opened for signature August 5, 1963. https://2009-2017.state.gov/t/avc/trty/199116.htm

Trends in Access to Computing Technology and Its Use in Chicago Public Schools, November 2007, Consortium on Chicago School Research at the University of Chicago. https://consortium.uchicago.edu/publications/trends-access-computing-technology-and-its-use-chicago-public-schools-2001-2005

U.S. Census Bureau. *Urban and Rural,* February 24, 2020. https://www.census.gov/programs-surveys/geography/guidance/geo-areas/urban-rural.html

U.S. Congress. House. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. HR 3162. 107th Cong., 1st sess. Congressional Record 147, part 14: 20400-20438. https://www.gpo.gov/fdsys/pkg/CRECB-2001-pt14/pdf/CRECB-2001-pt14-Pg20400-3.pdf.

U.S. Congress. Senate. Committee on the Judiciary, Federal Data Banks, Computers and the Bill of Rights: Hearings before the Subcommittee on Constitutional Rights. 92nd Cong., 1st sess., February 23, 24, and 25, and March 2, 3, 4, 9, 10, 11, 15, and 17, 1971.

U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Constitutional Rights. Federal Data Banks and Constitutional Rights: A Study of Data Systems on Individuals Maintained by Agencies of the United States Government. 93nd Cong., 2nd sess., 1974. Committee Print.

U.S. Congress. Committee on the Judiciary and Committee on Commerce. Surveillance Technology: Hearings before the Subcommittee on Constitutional Rights and the Special Subcommittee on Science, Technology, and Commerce, 94th Cong., 1st sess., June 23, September 9 and 10, 1975.

U.S. Congress. House. Committee on Interstate and Foreign Commerce. Subcommittee on Communications. Compendium of Papers Supplementing the Hearings on Telecommunications Research and Policy Development. 94th Cong., 2nd sess., 1976. Committee Print.

U.S. Congress. Committee on Indian Affairs. GAO Report on Tribal Access to Spectrum: Promoting Communications Services in Indian Country, 116th Cong., 1st sess., September 18, 2019.

U.S. National Archives and Records Administration. *Fred Hampton (August 30, 1948 - December 4, 1969)*, August 25, 2020.

Van DerWerff, Emily. "#Gamergate: Heres why everybody in the video game world is fighting." *Vox*, October 13, 2014. https://www.vox.com/2014/9/6/6111065/gamergate-explained-everybody-fighting

Van Dijk, Jan. *The Deepening Divide Inequality in the Information Society*. London: Sage Publications, 2005.

Van Dijk, Jan & Kenneth Hacker "The Digital Divide as a Complex and Dynamic Phenomenon." *The Information Society: An International Journal* 19 no. 4 (2003): 315-326. DOI: 10.1080/01972240309487

Van Deursen, Alexander and Jan A.G.M. Van Dijk. "Internet Skills and the Digital Divide." *New Media & Society* 13, no. 6 (2011): 893-911.

Virk, Kameron and Nest McGregor. "Blackfishing: The Women Accused of Pretending to Be Black." *BBC News*, December 5, 2018. https://www.bbc.com/news/newsbeat-46427180

Wacquant, Loïc. *Punishing the Poor: The Neoliberal Government of Social Insecurity.* Durham, North Carolina: Duke University Press, 2009.

Wahl, Jenny. “Legal Constraints on Slave Masters: The Problem of Social Cost.” *The American Journal of Legal History* 41, no. 1 (January 1997): 1-4. DOI:10.2307/845469

Wajcman, J. *Pressed for Time*. Chicago: University of Chicago Press, 2015.

Warschauer, Mark. T*echnology and Social Inclusion: Rethinking the Digital Divide*. Cambridge, Massachusetts: MIT Press, 2003.

Youn, S. “Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents.” *The Journal of Consumer Affairs* 43 (2009): 389-418.

Zhang, Mingliu and Richard Wolff. “Crossing the Digital Divide: Cost-Effective Broadband Wireless Access for Rural and Remote Areas.” *IEEE Communications Magazine* 42, no. 2 (2004): 99-105. DOI:10.1109/MCOM.2003.1267107

Zimmerman, Phillip. “Why I Wrote PGP.” *PGP User's Guide*, 1991. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

APPENDIX A: ETHNOGRAPHIC INTERVIEW QUESTIONS

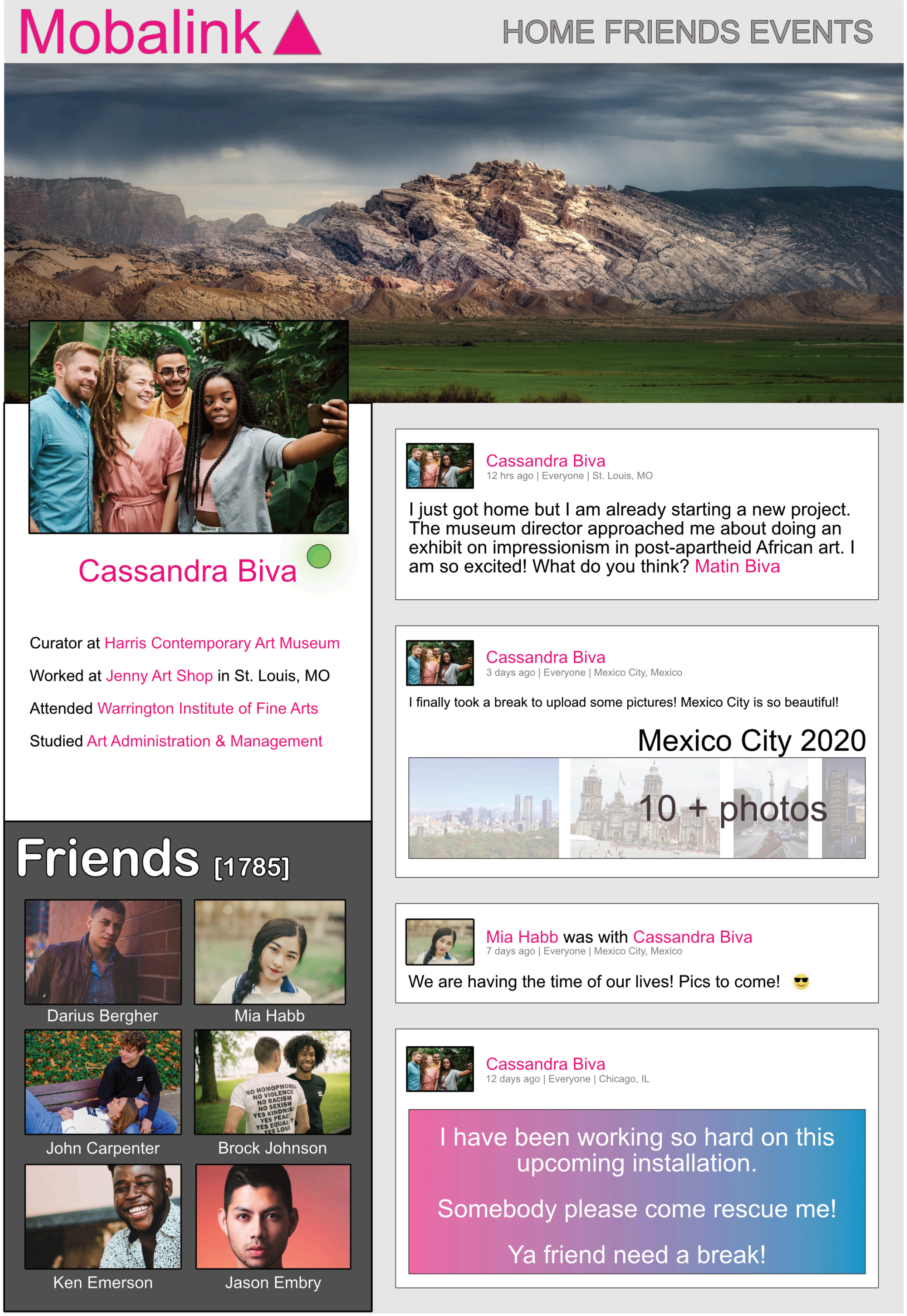
1. Would you like to participate in this recorded interview?
2. Please tell me about your daily computer use.
3. If someone says digital privacy, what is the first thing that comes to mind? Why?
4. Has someone ever viewed your digital content when your didn't want them to view it?
    1. What did you do to prevent it from happening again?
    2. Did you change your online presence or behavior?
    3. Who or what did you turn to for advice on preventing this from occurring again?
5. How safe do you feel in an online environment?
6. Please tell me about a time when you:
    1. Left and online platform
    2. Blocked someone online
    3. Second-guessed or restricted posting something online
    4. Used an online persona
7. What do you think of creators who post their entire lives online? Friend and family?
8. Do you think that school has prepared you or informed your decision making on digital privacy? If so, in what ways?
9. Who do you think worries about online privacy? Why?
10. What do you think of major data breaches?
11. Do you think your digital presence affects your ability to be successful after school?

The participants will participate in an online multi-stage one session interview conducted via Zoom or Skype. They will go through the following interview program in sequential order.

- Ethnographic interview (30 - 45 min): The participant will be asked predetermined open-ended questions by the Co-PI (Denavious Hoover). The questions will investigate their perceptions of privacy in the online environment and how they turn those perceptions into practice.
- Profile-Elicitation (4 profiles; one for each strategy) (5 - 15 min): Participants will be shown 4 completely fictitious social media profiles via screen-share. They will be asked to critique/analyze and provide general comments on the profiles. Participants will also be asked to compare and contrast the profiles on levels of privacy.
- Auto-Ethnographic Question (writing): Participants will be prompted with the following: "You are a stranger that has gained access to the whole of your online data without restriction. Describe what you see in one or more paragraphs." They will then be asked to write a paragraph or two describing their online presence from an outside positionality. The writing will be collected and become part of their interview response.

After participants have completed all three stages of the interview, the interview will end.

APPENDIX B: PROFILE-ELICITATION MATERIALS



Cassandra Biva

Curator at Harris Contemporary Art Museum

Worked at Jenny Art Shop in St. Louis, MO

Attended Warrington Institute of Fine Arts

Studied Art Administration & Management

Friends [1785]

Darius Bergher
Mia Habb
John Carpenter
Brock Johnson
Ken Emerson
Jason Embry

Cassandra Biva
12 hrs ago | Everyone | St. Louis, MO

I just got home but I am already starting a new project. The museum director approached me about doing an exhibit on impressionism in post-apartheid African art. I am so excited! What do you think? Matin Biva

Cassandra Biva
3 days ago | Everyone | Mexico City, Mexico

I finally took a break to upload some pictures! Mexico City is so beautiful!

Mexico City 2020

10 + photos

Mia Habb was with Cassandra Biva
7 days ago | Everyone | Mexico City, Mexico

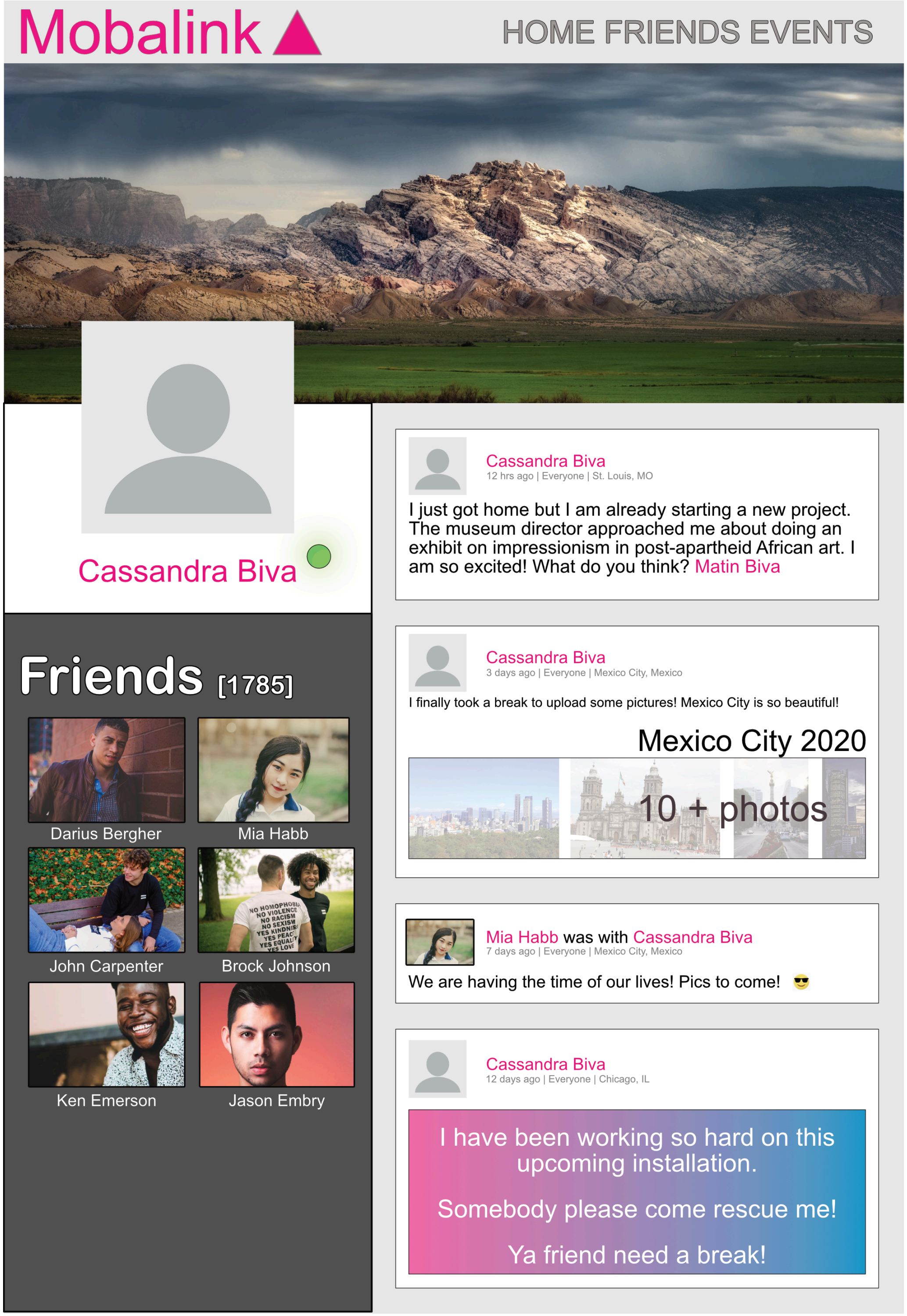
We are having the time of our lives! Pics to come! 😎

Cassandra Biva
12 days ago | Everyone | Chicago, IL

I have been working so hard on this upcoming installation.

Somebody please come rescue me!

Ya friend need a break!



Mobalink

HOME FRIENDS EVENTS

Cassandra Biva

Friends [1785]

Darius Bergher

Mia Habb

John Carpenter

Brock Johnson

Ken Emerson

Jason Embry

Cassandra Biva
12 hrs ago | Everyone | St. Louis, MO

I just got home but I am already starting a new project. The museum director approached me about doing an exhibit on impressionism in post-apartheid African art. I am so excited! What do you think? Matin Biva

Cassandra Biva
3 days ago | Everyone | Mexico City, Mexico

I finally took a break to upload some pictures! Mexico City is so beautiful!

Mexico City 2020

10 + photos

Mia Habb was with Cassandra Biva
7 days ago | Everyone | Mexico City, Mexico

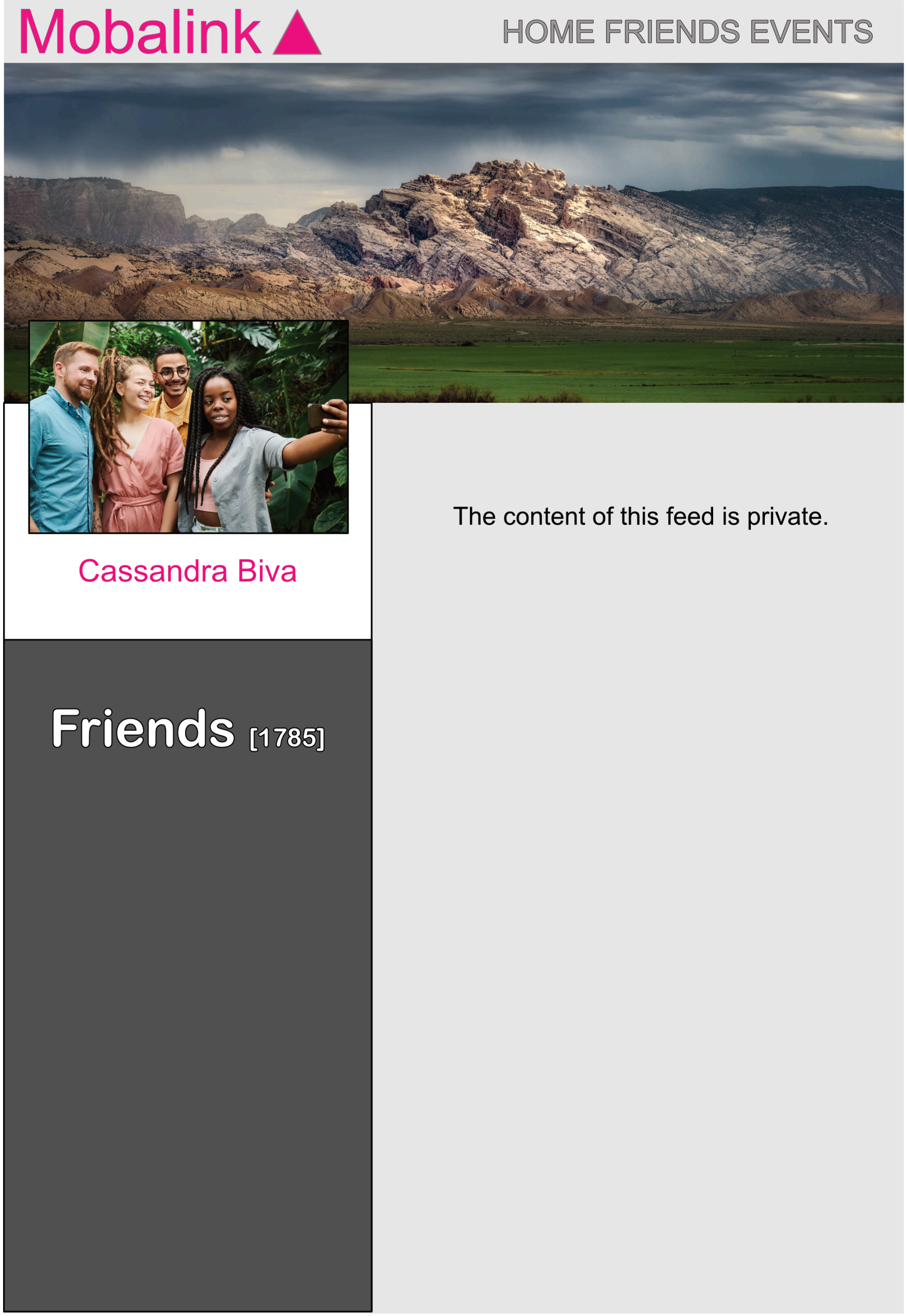
We are having the time of our lives! Pics to come! 😎

Cassandra Biva
12 days ago | Everyone | Chicago, IL

I have been working so hard on this upcoming installation.

Somebody please come rescue me!

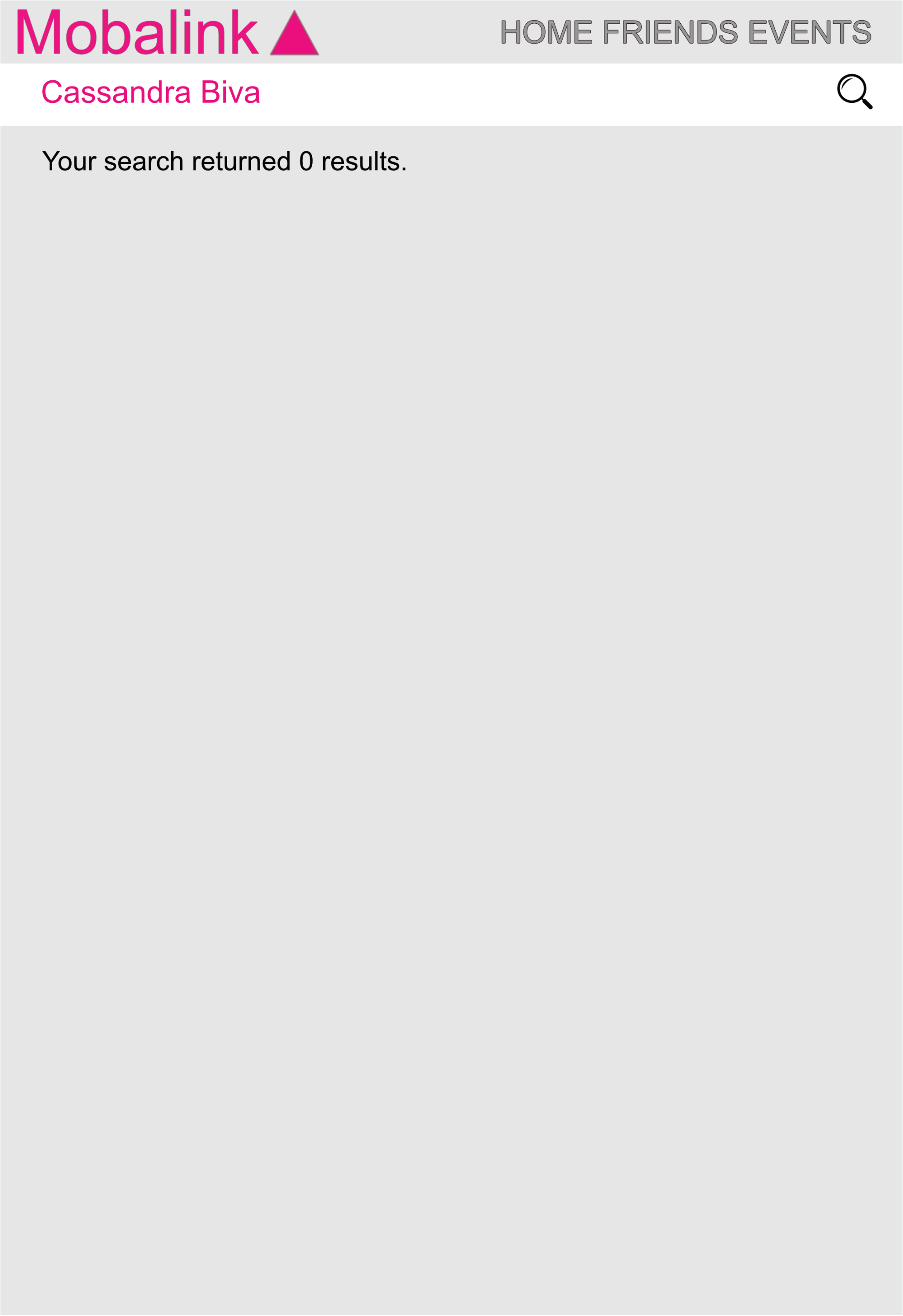
Ya friend need a break!



Cassandra Biva

Friends [1785]

The content of this feed is private.



Your search returned 0 results.