DON'T @ ME: SURVEILLANCE, SUBJECT FORMATION, AND THE DIGITAL INFORMATION ECONOMY

A thesis submitted to the faculty of

San Francisco State University

In partial fulfillment of

the requirements for

the Degree

Masters of Arts

In

Women and Gender Studies

by

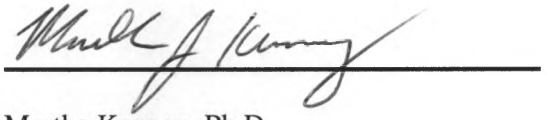
Riese Jordan Lin

San Francisco, California

Fall 2016

CERTIFICATION OF APPROVAL

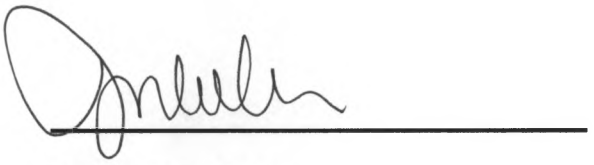
I certify that I have read *don't @ me: Surveillance, Subject Formation, and the Digital Information Economy* by Riese Jordan Lin, and that in my opinion this work meets the criteria for approving a thesis submitted in partial fulfillment of the requirements for the degree Master of Arts in Women and Gender Studies at San Francisco State University.



Martha Kenney, Ph.D.

Associate Professor

Women & Gender Studies



Julietta Hua, Ph.D.

Professor and Department Chair

Women & Gender Studies

DON'T @ ME: SURVEILLANCE, SUBJECT FORMATION,
AND THE DIGITAL INFORMATION ECONOMY

Riese Jordan Lin
San Francisco, California
2016

This thesis interrogates processes of digital subject production within the contemporary context of increasingly widespread and networked systems of U.S. state and corporate surveillance. Starting with an analysis of corporate datamining practices in mainstream social media spaces, I argue that users' digital consumptive labor undergoes processes of commodification that function to essentialize and perpetuate hegemonic constructions of identity categories. I then examine the ways in which the U.S. government deploys post-9/11 "war on terror" discourses to justify the use of biometric surveillance technologies and the appropriation of private sector surveillance data and resources as regulatory mechanisms in order to identify, isolate, and criminalize deviant and dissenting bodies while simultaneously producing docile, patriotic, and neoliberal digital subjects. Finally, I explore how this surveillant assemblage surrounding digital consumption, social media spaces, and the growing information economy produce essentialized notions of physical embodiment in ways that attempt to solidify categories of identity across gender, race, class, and ability; thereby foreclosing potential understandings of contextual, situated, and hybrid identities, subjectivities, and expressions, and limiting the possibility for social recognition and relationality across difference.

I certify that the abstract is a correct representation of the content of this thesis.

Chair, Thesis Committee

12/16/16
Date

TABLE OF CONTENTS

don't @ me: Subject Formation, Surveillance, and the Digital Information Economy

Introduction

This thesis interrogates processes of digital identity production and subject formation within the contemporary context of increasingly widespread and networked systems of U.S. state and corporate surveillance. Through examination of digital cultures, practices, and spaces, I will illustrate how neoliberal, capitalist, and nationalist ideologies influence the structuring of technologies in ways that aim to regulate users' digital and physical embodiments.

We live in an age where our relationships with digital technologies grow increasingly ubiquitous. More and more of our time is spent inhabiting digital spaces and surrounded by digital technologies. More and more of our lives are shared on social media; our smiling mugs are Instagrammed and thoughtfully filtered and tagged, our social connections are recorded and mapped out on Facebook—if a tree falls in the forest and no one is there to tweet about it, "screenshot or it never happened." When cars drive themselves and Google is old enough to be a teenager and our lifetimes of photographs are stored in ominous, ephemeral "clouds," it is more important than ever to ask what effects our intimate relationships with digital technologies have on our lives.

Drawing on the feminist theoretical tradition of analyzing subject formation, this thesis aims to put questions of subjectivity in conversation with our increasingly complex and ubiquitous relationships with technology. I draw from theorists including Judith Butler, Miranda Joseph, Joan W. Scott, and Evelyn Hammonds to explore the ways in which power operates in ongoing and overlapping digital relationships with different actors, such as corporate technology service providers, government institutions, law enforcement agencies, grassroots social movements, and finally, the users themselves. I look at a series of digital cultures and phenomena that characterize our current cultural landscape; these include #GamerGate and gendered cyberharassment in social media spaces; the digital information economy and covert government surveillance; *Pokémon GO* and augmented reality; and #BlackLivesMatter and digital worldbuilding. Through these discussions I illustrate inflections of power and influences of neoliberal capitalism, U.S. nationalism, and white heteropatriarchy in the disciplinary and regulatory structuring of modern communication technologies. I pose questions about how authority, epistemology, and knowledge production operate in relation to the digital, and ask how they might inform users' interactions with technological devices, within digital spaces, with state and corporate institutions, with other digital users, and ultimately, with their own conceptions of themselves.

Chapter one, "Digital Subjects," begins with an analysis of corporate datamining practices in mainstream social media spaces to demonstrate how digital user experiences and interactions are shaped and evaluated through lenses of neoliberal capitalism that in

turn delimit and reproduce the bounds of users' capacity for expression. I argue that users' digital consumptive labor undergoes processes of commodification that function to essentialize and perpetuate hegemonic constructions of identity categories, and foreclose upon the potential to understand identity as multilayered, intersectional, and contextually situated. I then examine different iterations of hashtag culture and the trend of commercial cooptation and corporate regulation to demonstrate how digital subjectivizing processes intended to regulate digital consumption do so at the expense of rendering nonnormative and deviant subjects vulnerable to cyberviolence.

In chapter two, "Palantir," I take a step back to consider the increasingly institutionalized entanglements between the U.S. state and the private sector that characterize our contemporary culture of digital surveillance. First, I examine the ways in which the U.S. government deploys post-9/11 "war on terror" discourses to justify the appropriation of corporate datamining resources and technologies in order to identify, isolate, and criminalize deviant and dissenting bodies and subjectivities. I then turn to a discussion of biometric technologies to demonstrate the parallels between digital and physical subjectivizing processes that take place under the disciplinary authority of this state and corporate surveillant assemblage.

Chapter three, "I Reject Your Reality and Substitute My Own," takes a final step back to identify and address the epistemological concerns that emerge when we consider the role of digital realities in shaping our physical realities, and vice versa. I draw from

several queer and feminist theoretical frameworks to analyze and deconstruct how we conceptualize authority, visibility, and intelligibility in relation to digital spaces and technologies, and trouble the binary notion that our digital and real lives are wholly separate and distinct. Finally, I speculate on potential strategies for users to queer and refigure our relationships with and within the digital in order to extend the terms of digital recognition and sociality in ways that understand and value subjects as complex, hybrid, situated, and relationally constituted.

Overall, my goal of this thesis is to draw a comprehensive picture that captures the role of "the digital" in shaping our modern world, and question how our conceptions of the digital play out in terms of knowledge production and meaning-making, especially for minoritarian, subaltern, or otherwise "deviant" subjects. How do our notions of the digital influence different aspects and interpretations of knowledge, of truth, of reality, and of sociality, both online and off? How do discourses surrounding the digital affect our overall understandings of the body, embodiment, and what it means to be human? How might we identify the regulatory and normalizing functions of the digital within processes of subject formation across categories of gender, race, class, ability, and nation, and what is required to resist its potentially violent, reductive, and subjugating effects?

Twenty-five years have passed since Donna Haraway first wrote in her "Cyborg Manifesto," "we are cyborgs. The cyborg is our ontology; it gives us our politics. The cyborg is a condensed image of both imagination and material reality, the two joined

centres structuring any possibility of historical transformation;"[1] and that "Cyborg writing is about the power to survive, not on the basis of original innocence, but on the basis of seizing the tools to mark the world that marked them as other."[2] It is my hope to continue Haraway's work of troubling and confounding boundaries between the physical and non-physical, the real and the digital, the human and the machine, reality and the imaginary. This thesis is my cyborg writing, my contribution to furthering our understandings of our cyberfeminist selves and expanding the potential for what we might conceive of as possible.

---

[1] Donna Haraway, "A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century," *Simians, Cyborgs, and Women: The Reinvention of Nature,* New York: Routledge, 1991, p. 150.

[2] Ibid., p. 171.

Chapter 1: Digital Subjects

In this chapter, I will attempt to articulate a notion of digital identity and subjectivity as produced and mediated by communication technologies and social media platforms within the greater context of the emergent digital information economy and its attendant cultures of datamining and corporate surveillance. I will first discuss how neoliberal capitalist ideologies influence the structuring of digital technologies that delimit the bounds of users' capacity for interaction and expression in social media spaces, which in turn functions as a subjectivizing mechanism to produce ideal digital consumer-subjects. I argue that our contemporary digital information economy prioritizes the maximal extraction of valuable personalized user data which, when read through hegemonic lenses, perpetuates the essentialization of identity categories and forecloses the potential for understanding identity as multilayered, intersectional, and contextually situated. I will then illustrate this subjectivizing process in practice by examining different iterations of hashtag culture, as well as its commercial cooptation and corporate regulation, to demonstrate how digital spaces constructed according to market logics can render nonnormative and deviant subjects dispossessed, unintelligible, and vulnerable to cyberviolence.

All Your Data Are Belong To Us

By "data" I am referring to any form of digital texts or information[1] disclosed by a user on a social media platform. "Metadata" refers to the paratextual information about that data, which can often be used to categorize and interpret the contents of that data. For example, say that I was feeling particularly dapper this morning and decided to take a selfie and share it on Twitter. The data in this case would include the contents of my tweet, namely the picture of my fine self and any caption I might have chosen to include. The metadata about my tweet includes my Twitter username, the tweet's date and timestamp, the geographical location from which I posted my tweet, as well as information about other Twitter users' interactions with my tweet—the number of times it was retweeted, favorited, or responded to, in addition to any metadata about those users' interactions. Although the data included in my tweet is in many ways "final"—upon its transmission I cannot go back and alter the contents of the tweet—the metadata about my tweet's circulation can continue to grow well past the time I hit "send." "Metadata" can also describe the information collected by Twitter's software that I communicated inadvertently through my interactions with and on Twitter, such as the wifi network or cellular tower I used to access the internet, the phone and operating system I used to take the photo, the internet browser or application I used to post the tweet, the number of times I revisited my tweet to check how many "favorites" my selfie

[1] In earlier drafts, I defined "data" as textual content or information *knowingly* published by a user, however, I recognize that user data can certainly be shared online without the user's volition.

earned throughout the day, and the recent websites and applications I happened to browse in between checking.[2] So often the information that social media corporations glean from users' interactions is widely undisclosed, and when it is, it is concealed behind vaguely-worded privacy policies and end-user license agreements that I am fairly certain nobody reads. Though I may not personally consider my narcissistic loading and reloading of my Twitter notifications as producing valuable data about myself, it is precisely the tracking of and trade in this type of behavioral data and metadata that drives the digital information economy and influences the ways in which digital spaces are structured.

The thing that makes social media spaces unique to other digital spaces is their overwhelming reliance on user-generated content. Facebook, Twitter, and YouTube do not create original media for user consumption; rather, they provide online platforms for users to publish and share media content with other users. Even though the majority of social media companies do not charge users for access to their services, they remain incredibly profitable from user-targeted advertising revenue. As New Media Studies theorist Aimee Morrison aptly puts it, "The users of Facebook are not its consumers but rather its product."[3] The aggregated user data and metadata surveilled and collected by social media companies like Facebook is packaged and sold to third-party advertisers, who in turn use that information to produce highly sophisticated and specific user-

---

[2] Twitter's Privacy Policy as of 27 January 2016, Accessed 17 April, 2016, https://twitter.com/privacy.

[3] Aimee Morrison, "Facebook and Coaxed Affordances," *Identity Technologies: Constructing the Self Online,* Madison, Wisconsin: The University of Wisconsin Press, 2013, p. 115.

targeted advertisements. In "The Political Economy of Privacy on Facebook," Christian Fuchs examines the ways in which Facebook derives profit from the commodification of its users' labor and data through a Marxist framework. Fuchs' analysis identifies two forms of user labor that take place in the context of Facebook. The first involves the production of original creative content and public communications between users, which can include uploading photos and videos, writing comments and status updates, and circulating silly memes. The second form of user labor is the production of less-public, individualized browsing data collected by Facebook when it surveils users' contacts and interactions, what pages they visit and the types of content they view, attention habits, and transaction histories. Fuchs argues that Facebook subjectivizes its users into "internet prosumers" (producer-consumers), whose digital consumptive behaviors produce and are translated into "information commodities" sold to third-party advertisers, which are in turn used to generate specifically targeted advertisements for users to consume.[4] Throughout this constant cycle of simultaneous production and consumption, Facebook accrues more and more user information in order to structure their user' experience in ways that maximize marketability, both of the user and of the advertising client:

> Facebook prosumers are double objects of commodification. They are first commodified by corporate platform operators, who sell them to advertising clients, and this results, second, in an intensified exposure to commodity logic. They are permanently exposed to commodity

[4] Christian Fuchs, "The Political Economy of Privacy on Facebook," *Television & New Media* vol. 13 no. 2, March 2012, p. 143-146.

> propaganda presented by advertisements while they are online. Most online time is advertising time.[5]

Facebook and other data-mining social media spaces commodify users' digital labor and sell them as user-specific consumer profiles that presume to represent users' identities in terms of niche marketable demographics. If user consumption can be understood as productive labor, in that it produces some form of reflexive knowledge or truth about a user's identity and consumption from which corporations can predict future consumption practices, then it is critical to consider the ways in which users' processes of consumption are always already situated within the context of digital capitalism.

Users = Consumers = Producers = Product

We can use Miranda Joseph's discussion of consumptive labor to expand our understanding of the productive properties of consumption and its attendant subjectivizing processes within the context of neoliberal capitalism. Joseph writes:

> Consumptive labor is procured and exploited through active subjection in the expression of needs, desires, self, identity, and community; as producers seem to freely sell their labor, consumers freely choose and purchase their commodities… In consumption, exploitation occurs insofar as by freely choosing, the consumer who is free of, short of, the means to meet her needs without choosing a commodity contributes to the accumulation of capital—and thus to the powers of the owners of the

[5] Fuchs, "The Political Economy of Privacy," p. 146.

> means of production—and enacts the cultural and social formations in which her choices are embedded but which she does not control.[6]

Joseph here is concerned with the construction of the consumer subject in relation to the capitalist producer. The consumer's identity and self-articulation in terms of consumption can only be expressed within the material (and in the case of my argument, digital) constraints that render certain forms of consumption possible. If we understand corporate social media providers as the owners of the digital means of production, that is, as the actors with power and control over the space in which consumptive digital user labor occurs, thereby producing commodifiable user data, then we can begin to see how digital spaces are structured around producing and regulating users into ideal consumer subjects. A digital subject's practices of consumption can only reflect aspects of their identity only within the bounds of intelligibility afforded by these digital spaces.

I am not arguing that one social media platform is more or less exploitative of its users' digital labor than another, nor am I arguing that a Facebook subject's potential for self-articulation is better or worse than that of a Twitter or Tumblr subject. Rather, regardless of the differential constraints across social media spaces, I argue that the processes of consumer subject production within the context of the digital information economy are structured around maximizing the extraction of valuable user data. Although we have no way of knowing exactly how users' personal data and consumption habits are

---

[6] Miranda Joseph, "The Performance of Production and Consumption," *Social Text*, 1998: 25-61. p. 43-44.

nefariously surveilled, collected, analyzed, and appraised by different social media companies, we can still witness the widespread prevalence of neoliberal capitalist ideologies normalized and embedded in a continuous feedback loop of users' performative digital consumption.[7]

A Series of Tubes

Thus far, I have only discussed the subjectivizing processes that take place in discrete, individualized social media platforms. Our understanding of digital subject production becomes even more complicated when we consider the ways in which users' social media profiles and data are becoming increasingly integrated across different social media services, platforms, and hardware. The option to "share" or "cross-post" information between a user's multiple social media accounts contributes to a sophisticated networking of data with the ability to draw connections between a user's presence and interactions in different online spaces that would, in earlier eras of the internet, have remained distinctly separate. For example, Facebook allows its corporate acquisitions and third-party affiliates to offer users the option to "Login with Facebook" in order to conveniently access their applications, websites, games, or online stores

[7] Although I want to resist making universalizing claims about corporate business and data mining practices in "social media spaces," considering that what we might recognize as "social media" today is subject to change, I feel comfortable making this particular generalization about contemporary dominant social media spaces due to the fact that of the top ten most trafficked social media platforms in early 2016, more than half are owned by either Google, Facebook, or Yahoo, all of which are companies whose trade is primarily based in information processing; see "Market Share of the Most Popular Social Media Websites in the U.S. in October 2016," *Statista*, October 2016, http://www.statista.com/statistics/265773/market-share-of-the-most-popular-social-media-websites-in-the-us.

without the pesky need to create a new service-specific account. In some cases, such as with the mobile dating application Tinder, users must have a Facebook account in order to access the service. Twitter "widgets" injected into the code of independent content producers' websites make it easy both for Twitter users to share links with the simple click of a "Tweet this!", as well as for Twitter to monitor its users' browsing habits that take place in the digital elsewheres of Twitter dot com. Another notable example is how Google tracks and consolidates its users' consumption of the company's myriad services, software, and devices, including Gmail, YouTube, Google Search, Google+, Google Chrome, Google Play, and the Google Chromebook, all under a single Google user account. Although these examples of cross-platform data sharing are usually connected with users' consent, some occurrences of cross-platform networked communications are purposefully kept hidden from consumers.

In March 2016, the advertising and marketing company SilverPush was exposed as covertly harvesting and selling user data via its "Unique Audio Beacon" (UAB) software.[8] SilverPush partners with applications and advertisers that use SilverPush's code to track consumers' exposure to and reception of advertisements across multiple devices. When a user sees an online advertisement associated with SilverPush on their computer, or watches a television commercial by a SilverPush advertiser, those

[8] Violet Blue, "Advertising's hottest surveillance software is surprisingly legal," *Engadget*, 25 March 2016, http://www.engadget.com/2016/03/25/advertisings-hottest-surveillance-software-silverpush.

advertisements use UAB software to emit an inaudible sound. If the user has a SilverPush-associated application installed on their phone or tablet, that application uses the device's microphone to detect the advertisements' UAB in order to collect user information in real time. Furthermore, SilverPush software runs in the background of applications and perpetually "listens" for UAB transmissions, even when the application in question is not in use, and always without notifying the user. According to SilverPush's co-founder Mudit Seth, Silverpush software can identify a user and their device "through 50 parameters, based on data collected through ad exchanges, app owners, and advertisers."[9] Conveniently, it is SilverPush's company policy to refrain from divulging which adverting companies and applications employ its surveillance software; however journalist Violet Blue has identified SilverPush software on both iOS and Android devices, and reports advertising contracts with companies including Google, Facebook, Twitter, Samsung, and Proctor & Gamble.[10] SilverPush is therefore able to collect personally identifiable user data from multiple networked sources in order to construct elaborate user-specific consumer profiles, consolidated and assessed for potential marketability, all without the user ever being made aware that such surveillance is taking place.

---

[9] Aparna Kalra, "Making the cookie crumble differently," *Business Standard*, 2 December 2013, http://www.business-standard.com/article/companies/making-the-cookie-crumble-differently-113120200046_1.html.

[10] Violet Blue, "Advertising's hottest surveillance software is surprisingly legal."

Setting aside for a moment the egregious violation of user privacy, consider the subjectivizing processes inherent in the consolidation of a user's multiple social media presences, digital interactions, and consumption practices into a single consumer profile. Essentially, everything we have ever done on the internet (or with, and in some cases near internet-enabled devices) is, in the end, refigured into making us better, faster, stronger and more profitable consumers, rather than Actual Human Beings, tweeting or tumbling as a form of self-articulation. I argue that the multi-sourced conglomeration of user data and metadata disposes of crucial meaningful context in order to force users into single, coherent, and essentialized consumer subjects rendered intelligible only according to market logics, thereby leaving no room for nuanced understandings or expressions of complex and situated identities and subjectivities.

#hashtags: A History

The rise of hashtag culture illustrates how user interactions are corporately co-opted to structure our digital worlds around extracting user labor such that we can only recognize users through lenses of consumption. As a result, users and identity expressions that fail to embody the ideologically "default" white heteronormative male user-consumer are rendered technologically dispossessed and vulnerable to cyberviolence.

The hashtag is an interesting example of a user-generated communication tool and culture that spontaneously emerged in digital space through user innovation before being

co-opted by corporate entities.[11,12] The hashtag (#) was "invented" as a search-friendly mechanism in the early years of Twitter, way before Twitter The Company figured out how to turn tweets into money, before corporate brands had "social media presences," and before "trending topics" and "promoted tweets" starting clogging up your timeline. Twitter's search function was inadequate back then, and some of the old-school Twitter users started putting pound symbols before key words and phrases, together called a "hashtag," in order to make their tweets more easily searchable and Twitter's search (previously and occasionally still done via Google's search function) more tolerable. Hashtagging tweets meant that the greater Twitter public could search *all* tweets posted to Twitter (not just the timeline of users they follow) for #breakingnews, #sportsballscores, #butts, or #LOSTtheories for the internet's most up-to-date, hottest takes on the world's happenings. Before Twitter even caught on to the unique communication tool that magically emerged out of user necessity, that would eventually #taketheinternet #bystorm #lol, seasoned Tweeters were already making hashtag #jokes like a #hashtag #baller.

But Twitter eventually did catch on to the hashtag trend, and most mainstream social media services followed. Twitter turned hashtags into clickable links, which was

---

[11] Disclaimer: This history of hashtags is entirely informed by my own observations and experiences with the emergence and growth of hashtag culture, usage, and history. In no way is this history of hashtags complete by any means, and different interpretations of the rise of hashtags surely exist out there. Please don't email me about this.

[12] For alternative histories on the #hashtag, see Liz Gannes, "The Short and Illustrious History of Twitter Hashtags," Gigaom, 30 April 2010, http://gigaom.com/2010/04/30/the-short-and-illustrious-history-of-twitter-hashtags.

#revolutionary—users could now interact with and browse #topics with a single click without needing to perform a self-guided search. However, Twitter's adoption and refiguring of hashtags for capitalistic means developed into a primary bullet of the long list of tweeters' grievances with how the social media space was and continues to be managed.[13]

It started with #TrendingTopics, a permanent sidebar listing the current, most popular ("trending") location-based hashtags that tweeters are tweeting about. At first, #TrendingTopics was a welcome addition to Twitter's user-experience, as it introduced hashtags into the widespread Twitter vernacular and influenced users to connect with and engage other tweeters about topics of interest. It wasn't long before #TrendingTopics became yet another excruciating marketing scheme and Twitter began promoting corporate hashtags as "trending,"[14] thereby covertly disguising advertisements as popular discussion topics (it is worth noting that Twitter also sells advertisements in the form of "Promoted Tweets," which are also disguised as Content That Users Actually Want To See and are considerably difficult to discern from actual tweets). We all know how users love a good hidden advertisement pretending to not be a hidden advertisement. Outside

---

[13] The garbage-fire-of-a-year 2016 not only brought about Twitter's "moments," or algorithmically promoted, non-chronological Twitter timelines that have the annoying effect of decontextualizing "Tweets You Might Like" and actively working against the instantaneous and ephemeral ambiance upon which the platform was founded; Twitter also killed Vine. R.I.P. Vine.

[14] Patricio Robles, "Twitter's latest ad experiment: paid trending topics," *Econsultancy*, 17 June 2010, https://econsultancy.com/blog/6099-twitter-s-latest-ad-experiment-paid-trending-topics.

the realms of advertising and profitmaking, however, Twitter the Company has been historically terrible to the point of negligence around addressing hashtag cultures on its platform that incite trolling, cyberviolence, and hate groups; the most notorious of which is #GamerGate.

Cyberviolence against women is not a new phenomenon. It is particularly not uncommon within the traditionally hypermasculine and heterosexist video games culture, community, and industry. A textbook example of gendered cyberviolence can be found in the case of Anita Sarkeesian, creator of the blog "Feminist Frequency," whose outspoken critique of hegemonic gaming culture attracted waves of ruthless online and offline harassment from an exceptionally whiny contingent of gamers. In May 2012, Sarkeesian launched and successfully funded a Kickstarter campaign to create *Tropes vs. Women in Video Games,* a video series aimed at deconstructing the heterosexist, misogynistic, and racialized representations of women in video games.[15] Despite the project's initial overwhelming support, Anita Sarkeesian was the victim of violent online harassment that included attempts to hack her e-mail and social media accounts; an assault of pornographic images in which Sarkeesian is depicted being raped by video game characters;[16] and the production of a game entitled *Beat Up Anita Sarkeesian* by Ben Spurr (@Bendilin), who created the game because, "She claims to want gender equality

---

[15] "Tropes vs Women in Video Games," *Kickstarter*, May 2012, https://www.kickstarter.com/projects/566429325/tropes-vs-women-in-video-games.

[16] Anita Sarkeesian, "Harassment via Wikipedia Vandalism," *Feminist Frequency*, 10 June 2012, https://feministfrequency.com/2012/06/10/harassment-and-misogyny-via-wikipedia.

in video games, but in reality, she just wants to use the fact that she was born with a vagina to get free money and sympathy from everyone who crosses her path."[17] Sarkeesian is only one victim of the widespread misogyny that permeates the gaming community, and that incites technological, psychological, and material violence against women. According to Sarkeesian:

> The online harassment epidemic also affects a great number of women... We have no idea how many women have been scared into silence, deleted their blogs, removed their videos or simply refrained from saying anything on the internet altogether – but I am certain it's a significant and depressing number. That has to change... Online harassment and abuse needs to be taken seriously by the companies and institutions that provide the infrastructure for our lives online.[18]

---

[17] *Beat Up Anita Sarkeesian* was removed from its original host site *Newgrounds* the day after its debut. Ben Spurr's author's note states, "Anita Sarkeesian has not only scammed thousands of people out of over $160,000, but also uses the excuse that she is a woman to get away with whatever she damn well pleases. Any form of constructive criticism, even from fellow women, is either ignored or labelled [sic] to be sexist against her." See "Eulogy for: Beat Up Anita Sarkeesian," *Newgrounds,* 7 May 2012, http://www.newgrounds.com/portal/view/598591/; Digitally assaulting popular culture celebrities is no new concept to the *Newgrounds* community; in fact, the website has an entire genre of independently-produced "Assassin" games: "It was the mid 90s, the dawn of the web and for the first time ever, THE PEOPLE had access to global media. One of the first ways we wielded our new-found power was by making games where you beat up and kill establishment celebrities"; "Assault," *Newgrounds,* http://www.newgrounds.com/collection/assassin.

[18] Sheena Lyonnais, "Anita Sarkeesian Responds to Beat Up Game, Online Harassment, and Death Threats on Stephanie Guthrie," *Toronto Standard,* 10 July 2012, http://www.torontostandard.com/industry/exclusive-anita-sarkeesian-responds-to-beat-up-game-online-harassment-and-stephanie-guthries-death-threats.

Sarkeesian's experience here reflects the prevalence of women's vulnerability to cyberharassment across digital spaces, and emphasizes the need to address issues and cultures of cyberviolence at the infrastructural level.

On August 16, 2014, the disgruntled ex-boyfriend of independent game developer Zoë Quinn published an angry blog post that falsely accused her of having a sexual relationship with several games journalists in order to garner positive reviews for her game *Depression Quest.*[19] Zoë Quinn responded to these accusations and critiqued the sexist rhetoric used as a strategy to demonize and discredit her, which incited even more hatred and abuse from online mobs organized on Reddit, 4chan, and GitHub,[20] which included, "spreading [her] personal information around, sending [her] threats, hacking anyone suspected of being friends with [her], calling [her] dad and telling him [she's] a whore, [and] sending nude photos of [her] to colleagues."[21] These trolls collectivized under the hashtag #GamerGate, coined by video game voice actor Adam Baldwin, and unifying around a militarized call for "ethical" gaming journalism that opposes the

---

[19] See "thezoepost," *Wordpress,* 16 Aug 2014, http://thezoepost.wordpress.com/; and Nick Wingfield, "Intel Pulls Ads From Site After 'Gamergate' Boycott," *New York Times*, 2 Oct 2014, http://bits.blogs.nytimes.com/2014/10/02/intel-pulls-ads-from-site-after-gamergate-boycott.

[20] Zoë Quinn, "Once Again, I Will Not Negotiate With Terrorists," *Quinnspiracy,* 19 Aug 2014. http://ohdeargodbees.tumblr.com/post/95188657119/once-again-i-will-not-negotiate-with-terrorists.

[21] Jesse Singal, "Gaming's summer of rage," *The Boston Globe,* 20 September 2014, https://www.bostonglobe.com/arts/2014/09/20/gaming-summer-rage/VNMeHYTc5ZKoBixYHzi1JL/story.html.

"corruption" of feminist critics, derogatorily named "Social Justice Warriors."[22] Their systematic harassment against Quinn also included SWATing, an act in which abusers would impersonate Quinn and report threats of violence to local law enforcement agencies, their intent being to trick law enforcement to send a SWAT team to arrest and/or harm her. Fearing that the daily death and rape threats would materialize into actual physical violence, Quinn was forced into hiding.[23] Quinn's experience struggling with different law enforcement and social media channels for recourse was often met with a general lack of technical knowledge and capability, or worse, an authority's disbelief and disavowal of responsibility.[24]

Quinn and Sarkeesian's experiences as women on the internet with opinions is nowhere near unique. They are also only two on the long list of female gamers terrorized under the #GamerGate banner.[25] Even now, over two years since the inception of #GamerGate, Quinn continues to receive daily harassment, often tweeting that "August

---

[22] Casey Johnston, "Chat logs show how 4chan users created #gamergate controversy," *ArsTechnica,* 9 September 2014, http://arstechnica.com/gaming/2014/09/new-chat-logs-show-how-4chan-users-pushed-gamergate-into-the-national-spotlight.

[23] Wingfield, "Intel Pulls Ads From Site After 'Gamergate' Boycott."

[24] Quinn, Zoë, "Why I Just Dropped The Harassment Charges The Man Who Started GamerGate," *Zoë Quinn//Unburnt Witch,* 10 Feb 2016, http://blog.unburntwitch.com/post/139084743809/why-i-just-dropped-the-harassment-charges-the-man.

[25] See Leigh Alexander, "But WHAT CAN BE DONE: Dos and Don'ts to Combat Online Sexism," 5 July 2014, http://leighalexander.net/but-what-can-be-done-dos-and-donts-to-combat-online-sexism/; and Brianna Wu, "No skin thick enough: The daily harassment of women in the game industry," *Polygon,* 22 July 2014, http://www.polygon.com/2014/7/22/5926193/women-gaming-harassment.

[2014] never ends."[26] #GamerGate can be seen as an example of how gendered violence on a social media platform can extend beyond digital cyberbullying, stalking, and trolling, and into threatening targets' real-life physical and psychological safety. Cyberviolence is such a real-life issue for non-ideal cybersubjects including women and people of color online that the United Nations' Broadband Commission on Digital Development published their concerns in a 2015 report, "Cyberviolence Against Women and Girls."[27,28] Even still, although they provide one of the tenuous digital battlegrounds in which digital harassment occurs, Twitter the Company cannot be fucked to intervene (let alone acknowledge their service's rampant bully problem), and #GamerGate trolls continue to troll without consequence and chase women off the internet.[29] Furthermore,

---

[26] Quinn, Zoë, "August never ends," *Zoë Quinn//Unburnt Witch,* 11 January 2015, http://blog.unburntwitch.com/post/107838639074/august-never-ends; @TheQuinnspiracy, 11 January 2015, https://twitter.com/thequinnspiracy/status/554427624248709120.

[27] The Broadband Commission of Digital Development was formed in 2010 through a partnership between the International Telecommunication Union and United Nations Educational, Scientific, and Cultural Organization (UNESCO). Though the Commission has its flaws (see next footnote), at the very least its existence indicates the international acknowledgement of feminized cyberviolence as a persistent and systemic problem.

[28] Zoë Quinn herself was one of a half-dozen victims of cyberviolence invited to the United Nations to evaluate and present this report. Her inclusion was tokenistic, however, and Quinn expressed disappointment at the Commission's top-down, market-driven strategy for addressing feminized cyberviolence that reflected the international community's widespread ignorance of the complex subjectivities of and critical security concerns for targets of online harassment. See Sarah Jeong, "'I'm Disappointed': Zoë Quinn Speaks Out on UN Cyberviolence Report," *Vice Motherboard*, 1 Oct 2015, http://motherboard.vice.com/read/im-disappointed-zoe-quinn-speaks-out-on-un-cyberviolence-report.

[29] The severe inaction on the parts of Twitter and other social media companies to address cyberviolence has inspired users like Zoë Quinn to organize user-generated, vigilante anti-harassment and anti-bullying task forces such as Crash Override Network, which I will discuss at greater length in chapter three.

Twitter's abuse-reporting system is incredibly lacking and victim-blamey[30] (a problem all-too-familiar on the majority of social media platforms), and involves an incomprehensive checkbox-style-fill-out-form better suited for identifying spam accounts. The only other option targets of cyberviolence have is to block the offending user(s)' accounts, which does nothing to prevent them from creating additional "sockpuppet" accounts and continuing the abuse (on Twitter, this is referred to as the "egg problem,"[31] but it is certainly a widespread issue across social media platforms[32]).

I argue that the severe lack of action on the part of Twitter to address its platform's immense harassment problem implicates Twitter as part of the problem, and part of the network of powerful (in)actors cultivating and perpetuating a normalized digital culture of gendered cyberviolence. This communicates to targets of cyberviolence that they are unwelcome and invalid and unvalued as users, that their experiences are not deserving of consideration, and that technology megacorporations have no interest in assuring that their digital spaces are safe spaces for all users.

---

[30] Twitter's abuse-reporting policy places the burden of proof onto the target of harassment. Requiring victims of cyberviolence to comb through and document tweets and messages from their abusers can be labor-intensive and psychologically triggering, which I argue functions to dissuade targets of harassment from reporting assholes in the first place. See Appendix: Figure 1.

[31] Twitter's default user avatar is an egg, so it is general knowledge that accounts lacking personalized avatars are usually secondary "sockpuppet" accounts, spam, or trolls.

[32] Appendix: Figure 2.

Figure 1: Tweet by @Sickayduh highlighting Twitter's fucked up priorities is retweeted over 20,000 times.[33]

Figure 2: @robfee's tweet suggests that Twitter is more concerned with protecting corporate interests rather than actual human people.[34]

[33] Tweet by @Sickayduh, 13 August 2016, https://twitter.com/sickayduh/status/764683140417728512.

[34] Tweet by @robfee, 21 August 2016, https://twitter.com/robfee/status/767606169430921216.

The widely-circulated tweets showcased in Figures 1 and 2 evidence tweeters' exasperation at Twitter The Company's willful ignorance of cyberviolence in comparison to its willingness to bend over backward to avail corporate interests. In these examples, Twitter is clearly more concerned with protecting corporate assets than maintaining a safe user base. As prosumer subjects, Twitter users are valued for their capacity for capitalist consumption, and this is given primacy over users' actual needs and self-interests—in this case, protection from harassment. Twitter's digital subjects retain value only to the extent to which their digital labor can be exploited; outside of market lenses, their subjectivity is rendered unintelligible.

#lesbians

The recent #lesbians debacle on Tumblr marks an even more explicit example the subjectivizing processes through which social media companies regulate the boundaries of their users' capacity for identity expression and community cultivation, thereby producing and reading user accounts through hegemonic lenses that obscure and erase deviant experiences and knowledges. On August 19, 2016, Tumblr, in a motion to crack

down on the site's infestation of porn-slinging spambots,[35] disabled the searchability of the #lesbian tag:

[35] Tumblr's "notes" sharing function is uniquely exploitable by spam accounts, as "reblogging" or "favoriting" other users' posts automatically creates a link back to the original account. Spam accounts use this link-back system to trick traffic-tracking algorithms such as those used by Google to appear as though they were highly trafficked and popularly referenced websites. Tumblr's rationale for disabling the #lesbian search term is presumably to avoid culpability (while maintaining a "family-friendly" consumer-facing veneer) in the event of a user falling victim to malicious software embedded in pornographic spam Tumblr posts tagged #lesbian.

Figure 3. A Tumblr conversation thread where lesbians discover and express outrage at their identity label being considered Not Safe For Work.[36]

[36]Screenshots from Tumblr thread (Origin: @transpolarized), http://lesbianzoidberg.tumblr.com/post/149198684374/lesbian-death-trope-transpolarized.

As user @transpolarized notes, Tumblr's decision to flag #lesbian appears contradictory to the social media's reputation for being particularly welcoming to queer users and communities. Often heralded as being a safe space for nonnormative identity exploration and expression,[37] it is rather surprising that Tumblr would make such a drastic decision to potentially alienate such a large demographic of its user base. Tumblr is an aesthetically-geared "microblogging" platform where users can manage one or more blogs ("tumblrs") and post images, videos, links, and short-form pieces of writing; often revolving around specified themes, ranging from Harry Potter fanfiction to personal hormone therapy journals to .gifs of foxes. The culture on Tumblr is that of curation, so there is a high emphasis placed on "reblogging," or re-publishing and sharing other users' posts on your own Tumblr, thereby incorporating other users' content into your own personal digital aesthetic. Hashtags are therefore a crucial part of Tumblr's user-experience, as it is and how users discover and stumble into other blogs, communities, and fandoms with shared interests and affiliations.

In rendering the #lesbian tag unsearchable, Tumblr is effectively erasing the "lesbian" "aesthetic" from the platform's accessible archive. Not only does this communicate the heterosexist idea that lesbians exist exclusively for sexualized objectification by the male gaze, but also that the complexity and diversity of the lesbian aesthetic and experience is entirely reducible to the realm of the sexual and pornographic.

---

[37] Alicia Eler and Brannon Rockwell-Charland, "Naming a Radical Queer Girl Tumblr Aesthetic," *Feminist Journal of Art and Digital Culture,* iss. 32., 2015. https://dpi.studioxx.org/en/no/32-queer-networks/naming-radical-queer-girl-tumblr-aesthetic.

What is at stake here is lesbian-identified Tumblr users' ability to participate in collaborative and co-productive meaning-making. As a continual act of self-articulation and re-articulation, participation within Tumblr's interface and culture via blogging and reblogging houses incredible potential to share in, revise, and build upon a constant circulation of ideas. The "lesbian Tumblr aesthetic" is in effect a digital world-making project wherein lesbian users cultivate different iterations of identity-based expression and desire through the relational reception, internalization, and reproduction of meaning around the hashtag #lesbian. Unfortunately, these potentially fruitful digital realities are hampered by Tumblr overseers' inability to conceive of #lesbians as having any value or definition apart from sexually exploitative girl-on-girl action for the benefit of patriarchal titillation. Actual Lesbians interested in connecting with Other Actual Lesbians are now denied a forum for sharing ideas, developing communities, or even finding one another. Meanwhile, porn blogs reign supreme:

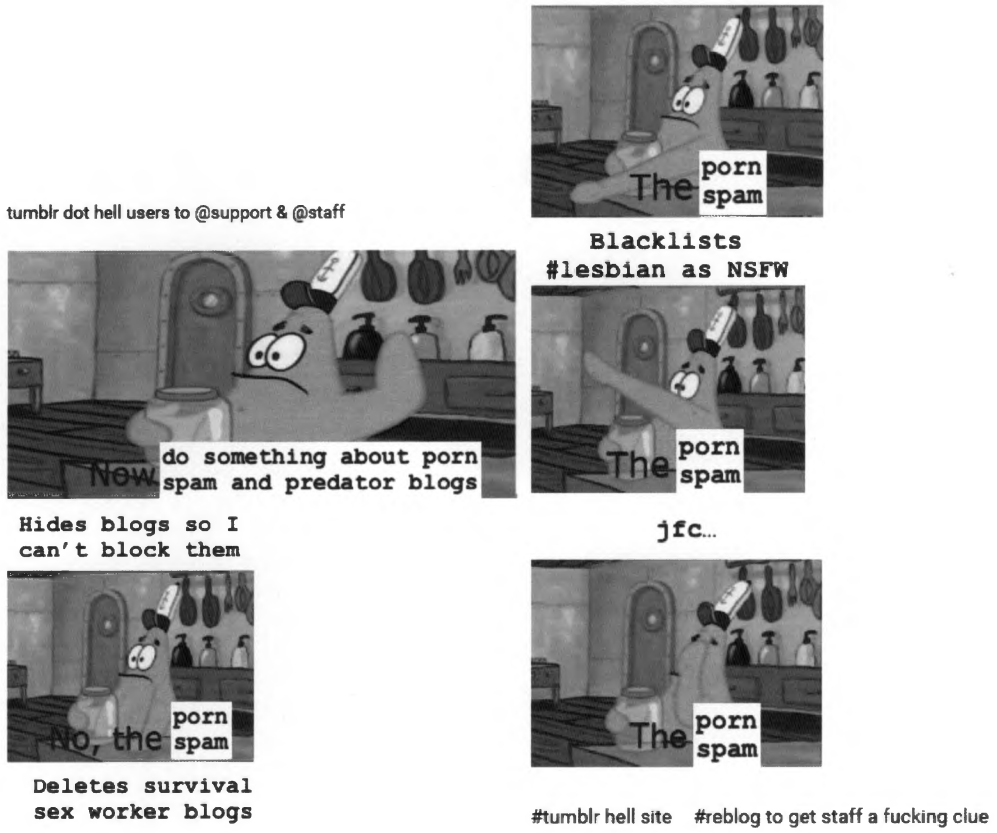


Figure 4. @venusisfortransbians expresses Tumblr lesbian discontent by referencing a popular internet meme featuring the lovable and occasionally challenged Patrick Starfish from the *Spongebob Squarepants* franchise.[38]

Tumblr has essentially deemed it more cost-effective and/or profitable to disable the #lesbians search entirely (thereby presumably avoiding any responsibility for user complaints regarding the site's bountiful explicit content) rather than address its rampant pornbot problem. Granted, considering how computer algorithms are not presently sophisticated enough to accurately and contextually identify sexually explicit content as

[38] Screenshot of original meme by Tumblr user @venusisfortransbians, "tumblr dot hell users to support staff," http://venusisfortransbians.tumblr.com/post/149200577599/tumblr-dot-hell-users-to-support-staff.

well as humans,[39] it is much easier and cheaper to block the entire #lesbian tag rather than combing through all accounts using the #lesbian tag, identifying spammy blogs, and deleting them individually. However, can't we all agree that it would be worthwhile for Tumblr—that Tumblr would be a much better Tumblr—if the company actually acknowledged and addressed the root of its porny spambot problem, with a ban-scalpel rather than a blanket band-aid, and let the real human #lesbians have their hashtag, their community, and their aesthetic back?

As a social media space, Tumblr has so much potential to allow users to create and explore different digital realities and means of expression through the rapid and constant circulation of images, texts, ideas, and "aesthetics." Tumblr's interface encourages identity production, self-articulation, and experimentation that is relationally co-productive; users' Tumblr accounts and archives are constant re-creations of digital selves composed of and maintained through blogged and reblogged user-generated and user-to-user content. In "Naming a Radical Queer Girl Tumblr Aesthetic," scholars Alicia Eler and Brannon Rockwell-Charland consider Tumblr "a space of safety, creativity, self-expression, and escape for young queer women and women of color… a utopic space for girls of all genders who regularly experience oppression for just being their selfies, who

[39] The age-old "Is it art or is it porn?" problem, "I'll know it when I see it," is notoriously difficult to accurately program computers to recognize; see Daniela Hernandez, "This is How Computers See Porn," *Fusion*, 30 June 2015, http://fusion.net/story/158507/this-is-how-computers-see-porn.

have to shift between multiple identities on a daily basis."[40] Eler and Rockwell-Charland celebrate Tumblr for enabling (mostly young) queer and women of color to express different identities and desires online without safety concerns, especially anonymously, as Tumblr only requires a username and private e-mail address (as opposed to services like Facebook which use a "Real Name Policy"[41]). Though on its surface Tumblr might look like a "safe space" where users' accounts are theoretically "anonymous," the authors here are only discussing user-to-user interactions and fail to consider the relationships between users and Tumblr itself, nor the market-driven context in which these relationships take place. Users' information is certainly not "anonymous" to Tumblr the Company, and users do not know the extent to which Tumblr (or its parent company, Yahoo, or Yahoo's parent company, Verizon, or any of the third-party affiliates to whom Tumblr sells information and advertising) collects and compiles user data, nor how it informs the algorithms Tumblr employs to populate user-specific, personalized digital worlds.

---

[40] Alicia Eler and Brannon Rockwell-Charland, "Naming a Radical Queer Girl Tumblr Aesthetic."

[41] Facebook's "Real Name Policy" has been critiqued by a number of queer and Native American users whose names are often flagged by Facebook's algorithm as "not real names"; see Aura Bogado, "Native Americans Say Facebook Is Accusing Them of Using Fake Names," *Colorlines*, 9 February 2015, http://colorlines.com/archives/2015/02/native_americans_say_facebook_is_accusing_them_of_using_fake_names.html/; Dana Lone Hill, "Facebook Don't Believe in Indian Names," 2 February 2015, http://lastrealindians.com/facebook-dont-believe-in-indian-names-by-dana-lone-hill/; and Abby Phillip, "Online 'Authenticity' and How Facebook's 'Real Name' Policy Hurts Native Americans," *Washington Post – Blogs*, 10 February 2015, https://www.washingtonpost.com/news/morning-mix/wp/2015/02/10/online-authenticity-and-how-facebooks-real-name-policy-hurts-native-americans.

Social media is undoubtedly changing the ways we communicate and the ways we relate, both to one another and to technology. Social media spaces also hold the potential to allow users to articulate digital selves whose influence extends beyond the boundaries of cyberspace and into our real-life understandings of our selves. Selfie-articulation, however, is only made possible within the limited frameworks upheld by the corporate behemoths that read value in marketable digital user labor—that is, if you haven't been cyberbullied off of Twitter or flagged as NSFW by Tumblr. Identity becomes data and users become digital subjects, acting the role of producer, product, and consumer; feeding into an endless, cycling network of service providers, devices, and platforms to show you better ads. In the industry they call it "improving services," though you're SOL if the service you want is a safe and accessible space for all users to freely communicate without fear of violence or censorship. *Especially* if it's not monetizable.

My next chapter will expand upon this discussion of digital user labor and data commodification through the additional lens of U.S. nationalism and government surveillance. I will explore the overlap between corporate technology producers and social media service providers in the private sector, and government and law enforcement institutions in processes of subject formation in relation to technology and digital spaces. Additionally, I interrogate the possible corporeal and embodied effects on different subjects that are a consequence of state and corporate influences on digital and technological infrastructure. In doing so, I hope to demonstrate how user and consumer relationships to the digital undergo regulatory functions of institutionalized power that

uphold and perpetuate not only economic subjectivizing processes, but political ones as well.

Chapter Two: Palantir

In previous sections, I discussed the ways in which users' interactions with and in digital technologies and spaces such as social media can be understood as form of labor commoditized by the private corporate entities that regulate technological consumption in order to collect user-specific data and metadata that is refigured for the purpose of developing targeted advertising and personalized user-experiences. This chapter will examine discourses surrounding the collection and surveillance of user data in order to illustrate the increasingly institutionalized entanglements between the U.S. state and the private sector that characterize our contemporary culture of digital surveillance. Through examination of post-9/11 "war on terror" sentiments circulating around and informing the U.S. government's domestic and international digital surveillance practices, as well as the state's conscription of private corporate technological resources, I hope to demonstrate how power and surveillance operate in digital space in order to identify and isolate gendered and racialized deviance and discipline users into neoliberal digital consumer-subjects. Looking at the Apple vs. FBI legal case following the late 2015 mass shooting in San Bernardino, California, I argue that we can witness the inheritance of PATRIOT Act-era cultural anxieties within the design of modern technologies that function to perpetuate hegemonic epistemological understandings of digital and physical embodiment.

The PATRIOT Act, PRISM, and You!

On June 6, 2013, Edward Snowden, a former contract worker for the United States' National Security Agency (NSA), leaked a series of top-secret documents revealing the existence of the NSA data-collection surveillance program, codename PRISM.[1] The formation of PRISM was enabled under President George W. Bush's USA PATRIOT Act, as well as the Protect America Act of 2007 and the later FISA Amendments Act of 2008 (upheld by President Barack Obama in 2012), all of which amended the Foreign Intelligence Surveillance Act of 1978 (FISA).[2] FISA established the Foreign Intelligence Surveillance Court (FISC), the judiciary which oversees the issuing of surveillance warrants to the various three-lettered U.S. intelligence agencies responsible for national security.[3] Section 702 of the FISA Amendments Act loosened the limitations on FISC oversight, permitting U.S. federal agencies to engage in warrantless electronic surveillance of non-U.S. foreigners abroad for up to a year without court approval. [4] According to the documents leaked by Snowden, the NSA's PRISM program has paid out millions of dollars to several high-level computer and telecommunication

---

[1] Ewan MacAskill, "NSA paid millions to cover Prism compliance costs for tech companies," *The Guardian,* 23 August 2015, http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

[2] Glen Greenwald and Ewan MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian*, 7 June 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[3] MacAskill, "NSA paid millions."

[4] Greenwald and MacAskill, "NSA Prism program."

companies including AT&T, Verizon, Facebook, Google, Microsoft, and Apple in return for access to data and metadata collected from their corporate servers.[5] The majority of these companies issued public statements denying their involvement with PRISM, [6] though the companies' ability to comment on such matters, especially considering their relation to "national security," were likely prohibited by federal nondisclosure gag orders.[7] Although the NSA's warrantless spying is legally supposed to be limited to foreign nationals and U.S. citizens suspected of collusion with threats to national security, the Snowden documents revealed that the NSA has "incidentally" collected and stored electronic data on millions of U.S. citizens' domestic communications in the form of text, emails, videos, and audio, and live search surveillance, as well as metadata ranging from location data to browsing and communication behaviors.[8] PRISM's "upstream" data collection method that intercepts electronic communications, allegedly in search of "national security threats," essentially casts too wide a net while fishing for "terrorists" that the technology captures unfiltered user data with no judicial oversight or

---

[5] MacAskill. "NSA paid millions."

[6] Ibid.

[7] Rebecca Grant. "Google tried to resist FBI requests for data, but the FBI took it anyway," *VentureBeat*, 6 June 2013, http://venturebeat.com/2013/06/06/google-tried-to-resist-fbi-requests-for-data-but-the-fbi-took-it-anyway.

[8] Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *The Washington Post*, 7 June 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

probable cause.[9] In fact, an analysis of leaked NSA documents conducted by *The Washington Post* found that *nine out of ten* data communications intercepted by PRISM were incidental, unintended targets of surveillance.[10] Considering these "behind-closed-doors," undisclosed, clandestine entanglements between the U.S. state and private corporations surrounding digital surveillance, user data, and national security, what effects do such entanglements have on users' identities and subjectivities?

Programming Patriotic Consumers

In "Monster, Terrorist, Fag: The War on Terror and the Production of Docile Patriots," Jasbir Puar and Amit Rai discuss post-9/11 "war on terror" discourses and the ways in which the circulation of such discourses function to produce "docile patriots" in opposition to the figure of the "terrorist other." This figure of the terrorist, coded as a monstrous, sexually deviant, and Orientalized subject of non-modernity, is deployed as a regulatory mechanism against which U.S. subjects must counter-identify in order to embody the patriotism and complicity demanded by the state to ensure their status as non-threatening subjects with national belonging.[11] Puar and Rai write:

---

[9] "How the NSA Domestic Spying Program Works," *Electronic Frontier Foundation*, accessed 26 February 2016, https://www.eff.org/nsa-spying/how-it-works.

[10] Barton Gellman, Julie Tate, and Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," *The Washington Post*, 5 July 2014, https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

[11] Jasbir K. Puar and Amit Rai. "Monster, Terrorist, Fag: The War on Terrorism and the Production of Docile Patriots," Social Text, 20.3 (2002): 117-148, p. 124-125.

> So that even if the long-time surveillance of African American and Caribbean American communities might have let up a bit after September 11, what we see is the legitimation and expansion of techniques of racial profiling that were in fact perfected on black bodies. If contemporary counterterrorism discourses deploy tropes and technologies with very old histories rooted in the West's own anxieties of otherness and normality, what transformations are we witnessing in the construction of the terrorist-monster? What innovations and reelaborations open new vistas to dominant and emergent forces in the hegemonic politics of the war on/of terrorism? The return of the monster today has enabled a multiform power to reinvest and reinvent the fag, the citizen, the turban, and even the nation itself in the interests of another, more docile modernity.[12]

I argue that the NSA and U.S. state's counterterrorism discourses, when applied to computer and information technologies and digital spaces, employ the figure of the "terrorist other" in order to construct a normalized "docile patriot" user who will willingly submit to state surveillance. The surveillant technological innovation of our present—the "counterterrorist" mechanism to keep us safe from monstrous deviance—now entails a networked system extending across digital and real spaces, monitoring users' digital and real lives. Further, when we consider the state and corporate entanglements evidenced by surveillance programs such as PRISM, the docile patriot subject produced and regulated under these hegemonic "counterterrorist" discourses and practices can be read as undergoing a doubled-docility, exposed not only to surveillance by the state but also to surveillance by private computer technology corporations. This

[12] Puar and Rai. "Monster, Terrorist, Fag," p. 139.

docile patriot is now also disciplined as a docile consumer in digital space, subject to regulation according to how different tech corporations judge their users' behaviors and interactions with and within digital technologies and spaces. Echoing Puar and Rai's discussion of surveillance technologies traditionally used to regulate and control black bodies, now additionally refigured based on post-9/11 anxieties anchored in Islamophobic fearmongering, the contemporary era of institutionalized digital surveillance extends into the personal information and metadata culled by corporations in order to decide which users, bodies, and digital consumption practices are considered "deviant," thereby justifying targeted surveillance and policing. Looking at the recent case of Apple, Inc. and the "FBiOS" can help illustrate this complex entanglement between the state and private corporations around the issues of digital surveillance, the "war on terror," and the construction of docile patriotic technology consumer-subjects.

FBiOS

On February 16, 2016, a federal court judge ordered Apple to assist the Federal Bureau of Investigation (FBI) in their investigation into the December 2, 2015 shooting in San Bernardino County, in which Syed Rizwan Farook and Tashfeen Malik engaged in a mass shooting and attempted bombing that killed fourteen people and injured twenty-two others.[13] Although initial investigations found no evidence that either Farook or

[13]Eric Lichtblau, "Judge Tells Apple to Help Unlock San Bernardino Gunman's iPhone," *New York Times,* 16 February 2016, http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html.

Malik were members of a terrorist cell or network, nor that they were being directed by the terrorist group recognized by the United Nations as the Islamic State,[14] President Barack Obama in an address to the U.S. nation declared the mass shooting an act of terrorism, and that Farook and Malik had "gone down the dark path of radicalization."[15] In the midst of their investigation, the FBI acquired Farook's password-protected iPhone 5c and an applicable warrant to search the phone, however its four-digit password protection software that, after ten failed password attempts would automatically wipe the hard drive, prevented the FBI from accessing the phone's data. Magistrate Judge Sheri Pym of the Federal District Court of Central California issued an order compelling Apple to assist the FBI's investigation by developing a method to "bypass or erase the auto-erase function."[16] Apple CEO Tim Cook responded in an open letter to Apple's consumers, expressing the company's intent to challenge the court order:

> We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone.

---

[14]Doug Stanglin and Kevin Johnson, "FBI: No evidence San Bernardino killers were part of a cell," *USA Today*, 5 December 2015, http://www.usatoday.com/story/news/nation/2015/12/04/suspects-family-shocked-killings/76773382.

[15]Barack Obama, "President Obama's full Oval Office Address," *CNN*, 7 December 2015, http://edition.cnn.com/videos/us/2015/12/07/president-obama-oval-office-terror-speech-full.cnn.

[16] Eric Lichtblau, "Judge Tells Apple."

> Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.
>
> The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.[17]

This "backdoor" that the FBI is requesting, colloquially "#FBiOS," would set an alarming precedent in the U.S. government's power and ability to conscript private corporations in their domestic surveillance operations; not to mention the unknown implications that FBiOS would have on the millions of Apple consumers outside the United States. Apple's motion to vacate the court order furthermore cites a number of California state and local officials in possession of hundreds of seized Apple devices with the intent to use FBiOS for cases completely unrelated to terrorism.[18] In all of these

---

[17]Tim Cook, "A Message to Our Customers," *Apple, Inc.*, 16 February 2016, http://www.apple.com/customer-letter.

[18]Part of Apple's defense insisted that, should the FBI's demand for access to Apple's technological resources be granted, there would be little recourse to prevent local Californian law enforcement from appropriating the tech to unlawfully access private user data from the hundreds of confiscated devices already in police possession. "APPLE INC'S MOTION TO VACATE ORDER COMPELLING APPLE INC. TO ASSIST AGENTS IN SEARCH, AND OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE," United States District Court: Central District of California, Eastern Division, 25 February 2016, https://www.documentcloud.org/documents/2722199-5-15-MJ-00451-SP-USA-v-Black-Lexus-IS300.html .

published statements, Apple is positioning itself as the consumer-friendly defender of privacy rights and information security. This is strikingly ironic, considering that Apple was one of the companies exposed as being involved with the NSA's PRISM surveillance project. Apple claims that the creation of FBiOS would pose a user security risk, especially if such a technology fell into the hands of "terrorists" or "malicious criminal hackers," but what security measures exist to protect Apple users from being spied on by Apple itself? Why is a "backdoor" only considered a "backdoor" when Apple is not in control?

It is hard not to read the company's actions as an elaborate marketing ploy.[19] This case against the FBI essentially gives Apple free media coverage, positioning the company as an industry leader in computer security and a benevolent advocate for technology consumers. Let us not forget that Apple, literally the largest, most valuable, and most profitable company on planet Earth,[20] has a single, primary capitalist objective—to sell computers and computer technologies (and the attendant mined user data) for profit. Consider the company's business model—creating generation after generation of new iPhones and computers produced with planned obsolescence in mind,

---

[19] Just days after the FBiOS news was released, Apple announced that the public unveiling of the company's next generation of iPhone and iPad would be rescheduled from March 15th to March 21st, the very day before Apple's scheduled court hearing against the FBI. See Arnold Kim, "Apple's Media Event to be Held the Week of March 21st, not March 15th," *MacRumors*, 27 February 2016, http://www.macrumors.com/2016/02/27/apple-event-march-21-week.

[20] Liyan Chen, "The World's Largest Tech Companies: Apple Beats Samsung, Microsoft, Google," *Forbes*, 11 May 2015, http://www.forbes.com/sites/liyanchen/2015/05/11/the-worlds-largest-tech-companies-apple-beats-samsung-microsoft-google/#18311ac6415a.

where the expectation is for consumers to ditch their older-generation devices for the latest and greatest line of tech that the company has to offer. For consumers lacking the economic capital to stay up-to-date with Apple's latest technologies and fulfilling their role as ideal consumers, their digital security becomes increasingly compromised.[21] This is not a simple matter of "just don't buy Apple products." When the market is controlled by a limited few monolithic tech corporations, all of which are implicated within the neoliberal state and corporate regime's digital surveillance, normal consumers have increasingly limited options when it comes to securing their data. User security will always come secondary to corporate profit.

The FBiOS case brings to light the dominant fearmongering discourses used to vilify constructed phantom "terrorist" "hackers" inherited from "war on terror" PATRIOT Act sentiments, and the deployment of such figures to rationalize contemporary domestic and international surveillance. The rhetorical strategy at work here—the positioning of Apple "versus" the U.S. government—detracts from the subjectivizing operations of power and technology underpinning this dispute; corporate and/or state actors deign themselves the innocent, trustworthy, objective arbiters of public and private, drawing and redrawing arbitrary virtual boundaries around which users,

[21]In particular, I am referring here to the constant, almost yearly cycle of newer and newer iPhone(x), iOS(x), and other device and update releases (a tech industry trend certainly not exclusive to Apple), without commensurate hardware and software support for older generations, thereby forcefully phasing out older products and their consumers from the market. For those unable to afford the latest supported devices and services, users and their data have limited technological capability and are more vulnerable to cyberattack.

which data, and which bodies are worthy and deserving of protection and of digital (and national) security. What's especially interesting is how Apple manages to publicly critique the FBI's overt surveillance, hypocritically aid the NSA with covert surveillance (as evidenced by Snowden's PRISM exposure), and simultaneously avoid acknowledging its own company's constant consumer surveillance. And by "interesting," I mean *not at all surprising*. What a time to be alive! Where users can live and internet surf in fear of their own government (not to mention "terrorists"!), but are not at all phased by and never call into question market-driven corporate surveillance.[22] As though our government and corporate overlords were not one and the same. As though that data was not used for the same violent ends. How far will our collective cognitive dissonance go to maintain the illusion of an artificial boundary between U.S. national security and the capitalist information economy, between the government and the digital "free" market, between our real worlds and selves and their cyber counterparts?

The U.S. State and Biometric Surveillance

In chapter one, I argued that corporate datamining practices endeavor to consolidate users' digital consumption practices into essentialized categories of identity evaluated and rendered legible according to capitalist market logics. I argue that we can witness similar essentializing processes of subjectification when we extend this analysis to state and corporate uses of biometric surveillance technologies. In the same way that I

[22] Wake up, sheeple!

emphasized the importance of questioning the epistemological framework through which users' digital data is analyzed, organized, and evaluated, we also need to consider what types of knowledges inform the development and implementation of biometric technologies, as well as the ways in which surveilled data is collected and used. Much like the ever-networked corporate systems of datamining mechanisms algorithmically essentializing and regulating identity, biometrics represent one of the clearest extensions of digital subject production into our physical, lived realities.

In *When Biometrics Fail: Gender, Race, and the Technology of Identity,* Shoshana Amielle Magnet analyzes a number of biometric identification technologies ranging from facial recognition software to digital fingerprint and retina scanners and finds that such technologies disproportionately misread or fail to recognize the bodies of women, people of color, and people with disabilities. Magnet terms these misreadings "biometric failure," and attributes cause not only to the use of the unmarked, "neutral" able-bodied white male as the default referent against which human bodies are read, but also the assumption that identities, bodies, and embodiment are wholly legible, static, and unchanging. Magnet writes:

> Biometric systems of categorization have the potential to exclude both those who don't belong to the privileged category and those whose body is illegible... Here we see the possibility for rendering othered bodies illegible to the biometric scanner in ways that may have serious implications for people's freedom and mobility... Although biological understandings of race and gender have long been analyzed by cultural

> theorists and scientists, their findings have largely failed to make it into the labs of scientists designing biometric systems. Biometrically producing reified racialized and gendered identities can have severe material ramifications. Most at risk from having their race, sex, and gender identities biometrically codified are those who refuse neat categorizations as well as those whose bodies the state believes to be a threat.[23]

Biometric attempts to read identity based on digital interpretations of the body not only resort to biologically essentialist understandings of identity, but further reify such understandings by effectively inscribing meaning onto the corporal body. For non-ideal, deviant, or otherwise biometrically unintelligible subjects, ascribing to such readings of identity and the body can have disastrous material repercussions, especially when it informs U.S. state surveillance practices. Digital readings of the corporeal body, as well as the epistemological errors and discrepancies therein, pose real-life consequences for nonnormative subjects in ways that necropolitically foreclose recognition of their realities and experiences according to hegemonic notions of what the body is and which bodies are worth protecting.

Lisa Marie Cacho writes in *Social Death: Racialized Rightlessness and the Criminalization of the Unprotected* about how discourses of "terrorism" and "illegality" have historically circulated within the U.S. national imaginary as a form of biopolitical control that inscribes criminalization onto gendered and racialized bodies, thereby

---

[23]Shoshana Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity,* Duke University Press Books: 2011, p. 45-48.

justifying racial profiling, discriminatory legislation and incarceration, police violence, and military aggression. In particular Cacho discusses how, domestically and currently, "illegality" is grafted onto immigrant Latina/o, Arab, and Muslim bodies, while simultaneously displacing the burden of performing "non-criminal," "non-terrorist," and "patriotic citizen" proof onto these suspect bodies.[24] In "Artful Concealment and Strategic Visibility: Transgender Bodies and U.S. State Surveillance After 9/11," Toby Beauchamp discusses the ways in which U.S. state surveillance regarding counterterrorism measures and matters of national security, although not outwardly intended to target transgender and gender-nonconforming people per se, is bolstered by a network of institutions that criminalize and pathologize gender deviance and transgression, thereby producing the transgender subject and body as deceptively threatening to the security and stability of the nation. Beauchamp writes:

> The monitoring of transgender and gender-nonconforming populations is inextricable from questions of national security and regulatory practices of the state, and state surveillance policies that may first appear unrelated to transgender people are in fact deeply rooted in the maintenance and enforcement of normatively gendered bodies, behaviors, and identities. I argue here that transgender and gender-nonconforming bodies are bound up in surveillance practices that are intimately tied to state security, nationalism and the "us/them," "either/or" rhetoric that underpins U.S. military and government constructions of safety. At the same time, the primary strategies and responses offered by transgender advocacy

[24] Lisa Marie Cacho, *Social Death: Racialized Rightlessness and the Criminalization of the Unprotected*, NYU Press: 2012, p. 103-105.

> organizations tend to reconsolidate U.S. nationalism and support the increased policing of deviant bodies.[25]

Rather than opposing the invasive (and transphobic) surveillance measures by the U.S. state, Beauchamp argues that transgender advocacy groups actually reify the state's policing of normatively gendered bodies by emphasizing "strategic visibility," that is, formal self-disclosure of transgender status through the state-recognized institutions such as the medico-legal system in order to appear to state officials as compliant and non-threatening subjects.[26] Implicit in this neoliberal responsibility of self-disclosure in order to produce oneself as the patriotic, ideal, and non-threatening transgender subject is a dichotomous distancing from otherwise "deviantly" gendered, racialized, and sexualized bodies coded as potentially dangerous terrorists, thereby justifying heightened levels of surveillance.[27] Essentially, the contemporary culture of U.S. state surveillance calls for gender-nonconforming bodies to self-disclose and render themselves visible, docile, and compliant with state surveillance, lest they risk appearing as though they have something to hide.

Through this example of airport security we can witness the subjectivizing processes of biometric digital technologies and their effects on the corporeal body in that they function to regulate the production of an ideologically normative concept of an

---

[25] Toby Beauchamp, "Artful Concealment and Strategic Visibility: Transgender Bodies and U.S. State Surveillance After 9/11," *Surveillance and Society* 6(4) (2009):356-366, p. 356-357.

[26] Ibid., p. 362

[27] Ibid., p. 363-364.

intelligible human "body," forcing deviant or subaltern bodies and embodiments to contort themselves in order to appear recognizably intelligible. Forced to appeal to digitized notions of an appropriately visible and readable human subject as coded into biometric technologies, subaltern subjects' neoliberal assimilation to "proper" embodiment as a strategy for survival additionally serves to perpetuate and reinforce the already limited and inaccurate digitized "misreadings" of what does and does not count as a viable body. For the transgender subject faced with biometric airport security, they are expected to successfully perform and embody either masculinity or femininity according to binary gender expectations in order to be visibly recognizable. At the same time, they must also be readily prepared to embody and be read as an intelligibly transgender "other" by willfully (and perhaps shamefully) rendering public a certain "wrongness" about their body—as though it is not the fault of binary societal gender expectations that reductively sort human bodies cleanly into two distinct categories of gender—thereby forcing the transgender subject to appear non-threatening by validating the authority of that same violent, exclusionary gender binary and its attendant reductive binary-gender-reading biometric machine.

Regulating Digital Embodiment

It is undeniable that the U.S. state employs biometric technologies, both implicitly and explicitly, to surveil, target, and kill unwanted bodies. Whether it takes the form of

hidden audio recording,[28] stingray[29] and predictive policing,[30] and covert drone surveillance of low-income communities of color domestically,[31] or civilian-murdering drone bombings with increasing regularity abroad;[32] the necropolitical abuse of violent technologies at every level of government is exercised to produce certain subjects as bodies worthy of state protection from the threat of and at the expense of all others. We already know that this surveillance is happening IRL. The FBiOS debate brought into the public discourse the state's unabashed intention to creep its way into our digital lives by appropriating corporate resources.

---

[28]"FBI agents hid microphones inside light fixtures and at a bus stop outside the Oakland Courthouse without a warrant to record conversations, between March 2010 and January 2011"; Jackie Ward, "Hidden Microphones Exposed As Part of Government Surveillance Program in the Bay Area," *CBS SF Bay Area*, 13 May 2016, http://sanfrancisco.cbslocal.com/2016/05/13/hidden-microphones-exposed-as-part-of-government-surveillance-program-in-the-bay-area.

[29]According to the American Civil Liberties Union, 66 local, state, and federal agencies in 24 states have been found using stingray tracking devices, or technology used to imitate cellular towers and collect location and identifying information from nearby cell phones. American Civil Liberties Union, "Stingray Tracking Devices: Who's Got Them?" accessed 17 May 2016, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them.

[30] National Institute of Justice, "Predictive Policing," 9 June 2014, http://www.nij.gov/topics/law-enforcement/strategies/predictive-policing/Pages/welcome.aspx.

[31]American Civil Liberties Union, "Domestic Drones," accessed 17 May 2016, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones.

[32]The Bureau of Investigative Journalism, an independent research firm based out of City University London, has monitored known U.S. drone attacks in Pakistan, Somalia, Yemen, and Afghanistan, and reports over four hundred airstrikes under the Obama administration alone, amounting to nearly four thousand casualties including at least five hundred civilians; see The Bureau of Investigative Journalism, "Covert Drone War," last modified 18 May 2016, https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs.

Although the FBI dropped its case against Apple in late March 2016, [33] I don't suggest we recycle our tinfoil hats just yet. The U.S. government continues to pursue other legislative[34] avenues to get into our e-mail inboxes[35] and Twitter feeds in order to criminalize, incarcerate, and murder people they don't like. In the midst of the FBiOS media shitstorm, the *New York Times* reported on the Obama administration's intention to pass policies that would formalize the use of NSA resources for domestic policing.[36] Previously, there was at least a subtle attempt to hide the NSA's sharing of warrantlessly-surveilled information having nothing to do with "terrorism" or "national security" with other government agencies including the Drug Enforcement Agency (DEA) or the

---

[33] According to lawyers representing the Justice Department, "The government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple Inc." However, information regarding the technique used to unlock Farook's phone remains "classified"; Danny Yadron, "San Bernardino iPhone: US ends Apple case after accessing data without assistance," *The Guardian,* 20 March 2016, https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone.

[34] ... And, let's be real, the federal government is also pursuing non-legislative (by which I mean, illegally and without telling us) avenues for surveillance (see next footnote).

[35] In October 2016, Yahoo's security team discovered a custom software surveilling hundreds of millions of Yahoo mail accounts, and suspected malicious hackers were responsible. It was later revealed that Yahoo's own engineering team bypassed their security team and programmed the spying software into the company's internal code at the request of the NSA and FBI. These events led to the resignation of Yahoo's Chief Information Security Officer, who is now in charge of security at Facebook; Joseph Menn, "Yahoo secretly scanned customer emails for U.S. intelligence," *Reuters*, 4 October 2016, http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT.

[36] Charlie Savage, "Obama Administration Set to Expand Sharing of Data that NSA Intercepts," *New York Times,* 25 February 2016, http://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html.

Internal Revenue Service (IRS).[37] At the South by Southwest (SXSW) conference on March 12, 2016, President Obama delivered a keynote addressing Silicon Valley and the greater tech community, urging cooperation with U.S. law enforcement:

> The question we now have to ask is, if technologically it is possible to make an impenetrable device or system, or the encryption is so strong that there is no key, there is no door at all, then how do we apprehend the child pornographer? How do we solve or disrupt a terrorist plot? What mechanism do we have available even to do simple things like tax enforcement? ... There has to be some concession to the need to be able to get into that information somehow.[38]

Though President Obama tosses around the moral-panic figures of the "terrorist" and "child pornographer" to justify streamlining the government's abuse of corporate surveillance technologies, he insists that he is "way on the civil liberties side of this thing."[39] Furthermore, he cautions that without hasty cooperation, "What you'll find is that after something really bad happens, the politics of this will swing, and it will become sloppy and rushed and it will go through Congress in ways that have not been thought

---

[37] Radley Balko, "Surprise! NSA data will soon routinely be used for domestic policing that has nothing to do with terrorism," *The Washington Post,* 10 March 2016, https://www.washingtonpost.com/news/the-watch/wp/2016/03/10/surprise-nsa-data-will-soon-routinely-be-used-for-domestic-policing-that-has-nothing-to-do-with-terrorism.

[38] Megan Collyer, "Watch President Barack Obama's 2016 SXSW Interactive Keynote," 12 March 2016, http://www.sxsw.com/interactive/news/2016/president-obama-sxsw-keynote-video.

[39] Ibid.

through, and then you really will have dangers to our civil liberties."[40] Is that a threat, Mister President? It appears the government's appropriation of corporate data and resources has never been a question of *if*, but rather *when*, and *with how much resistance*?

It would be misleading to frame Apple or any of the other corporate tech leviathans as users' benevolent savior from invasive state surveillance, especially when the state and private sector share a similar goal—to identify and profile tech users in order to more effectively control and regulate their bodies and actions, both online and off. It would also be misleading to pretend that the United States' government and its largest tech corporations aren't playing for the same team.[41] Instead, they together form the surveillant assemblage of digital and biometric technologies grounded in essentialized notions of identity and embodiment that attempt to solidify categories of gender, race, class, and ability, and permanently graft them onto the (allegedly intelligible) corporeal body. Combined with post-9/11 "war on terror" discourses as justification, the culture and technologies of surveillance function as regulatory mechanisms that identify, isolate,

---

[40] Collyer, "President Barack Obama's 2016 SXSW Interactive Keynote."

[41] Apple is arguably one of the largest beneficiaries of the United States' neoliberal economic policies that promote outsourcing manufacturing labor overseas and federal tax loopholes. According to *The Guardian*, between 2008 and 2014, Apple received over 21 billion dollars in tax breaks, stored 181 billion dollars in offshore subsidiaries, and spent 16 million dollars on lobbying the federal government. Apple comes first amongst the top ten highest grossing U.S. companies with offshore holdings in tax havens, which also include Microsoft, Google, and IBM; Rob Davies, "US corporations have 1.4tn hidden in tax havens, claims Oxfam report," *The Guardian*, 14 April 2016, http://www.theguardian.com/world/2016/apr/14/us-corporations-14-trillion-hidden-tax-havens-oxfam.

and criminalize deviant and dissenting bodies while simultaneously producing docile, patriotic, and neoliberal digital subjects.

In this chapter I combined queer and feminist theoretical frameworks critical of nationalism, neoliberalism, and capitalism in the context of contemporary digital surveillance to identify the disciplinary and subjectivizing functions on users and their physical and digital embodiment(s). My next and final chapter will delve further into the epistemological ramifications[42] of our corporate nation-state's digital surveillance on our very understandings of the body, embodiment, and reality itself to consider strategies for resisting and refiguring the gendered, ableist, and racially essentializing hegemonic influences over our relationships with and within digital technologies and spaces.

[42] To say "corporate brainwashing" feels like an exaggeration, but less so in a footnote.

Chapter Three: I Reject Your Reality and Substitute My Own

I was on the internet back when you could still be a dog on the internet.[1] I was a wee lad in the mid-90s, and I grew up surrounded by tech. My father used to own a computer retail and repair company, back before Apple and M$ were the only names in the game. I remember the first day he brought home a Nintendo 64 gaming console—*Turok: Dinosaur Hunter* (1997) was the first video game I ever played, and twenty years later I'm sure I still probably suck at shooting raptors with a bow and arrow. I remember my first Geocities website (look it up, kids!), back when we still called them "homepages," and mine was almost entirely devoted to Los Angeles Lakers fangirlery, dressed to the nines with flaming letters and ooga chaka baby .gifs. I was a catfish[2] on AOL Kidz Chat[3] before there was a word for or concept of "catfishing" and its attendant negative connotation. I was seven. I remember playing make-believe, A/S/L'ing[4]

---

[1] "On the Internet, nobody knows you're a dog" is an adage from the 1993 comic by Peter Steiner, originally published in *The New Yorker*. See Appendix: Figure 3.

[2] Urban Dictionary, a user-generated slang dictionary loosely recognized as an authority on hip lingo used by kids these days, defines a "catfish" as "someone who pretends to be someone they're not using Facebook or other social media to create false identities, particularly to pursue deceptive online romances"; Entry on "catfish," *Urban Dictionary,* accessed November 2016, https://www.urbandictionary.com/define.php?term=catfish.

[3] AOL Kidz Chat was a human- moderated chatroom (back in the pre-algorithmic chatbot age) provided by America Online Inc. (AOL), a telecommunications and media company that provided home computer users some of the earliest access to dial-up internet service in the 1990s. AOL Kidz Chat was a space primarily for AOL consumers' children and teens to connect and chat with others in a chaperoned context, back when it was *totally normal* to engage with strangers on the internet, before we had a concept of internet crime, online identity theft, or the nefarious, modern-day-boogie-man Craigslist Creeper.

[4] Age/Sex/Location, or A/S/L, was a common ice-breaking introduction in the early days of mass-internet-anonymity, and was used (and occasionally fictionalized, in my, and I'm sure many others', cases) to get a quick idea of the strangers in your immediate digital vicinity.

strangers left and right, and being whomever and whatever I felt like at the moment. I remember typing in every bad word my young mind could muster into chatboxes of all sorts, probing and trying to push past the discursive boundaries of chatrooms, seeing just how far I could go before a chatbot moderator would reprimand, mute, and kick me.

What I'm trying to say is, I care about tech. I care a whole fucking lot. Video games and the World Wide Web have always been my most beloved avenue for escapism, for imagination, and for playing with performativity before I ever knew that was a thing. I care about this stuff because I care about creating new worlds, finding new possibilities, and seeking out new forms of expression, representation, and recognition. But neoliberal corporate capitalism and government surveillance are harshing my mellow, hear?

I started out wanting to write my master's thesis about video games. In undergrad, I did a ton of research on queer and womens' representations in video games. But by the end of my first semester as a graduate student, I had begun to grow tired of cultural critique,[5] and my attention was drawn to the #GamerGate shitshow blowin' up my Twitter feed. My interest in video games grew to contain not only the textual content of

---

[5] See Lisa Nakamura, *Cybertypes: Race, Ethnicity, and Identity on the Internet,* New York: Routledge, 2002, and *Digitizing Race: Visual Cultures of the Internet*, University of Minnesota Press, 2008; Anita Harris, ed., *All About the Girl: Culture, Power, and Identity,* New York: Routledge, 2004; Knut Lundby, ed., *Digital Storytelling, Mediatized Stories, and Self-representations in New Media,* New York: Peter Lang, 2008; and Adrienne Shaw, "Do You Identify as a Gamer? Gender, Race, Sexuality, and Gamer Identity," *New Media & Society* 14, no. 1 (2012): 28-44, and "Putting the Gay in Games Cultural Production and GLBT Content in Video Games," *Games and Culture* 4 (3) (2009): 228-253.

video games, but also the gamer culture surrounding their production, circulation, and reception. My questions were no longer "Who and what do we make games about?" but rather, "Who decides who and what we make games about?" and more broadly, "*Who decides?*"

Like I said before, video games—and more broadly, online digital spaces in general— have always been my go-to escape from reality.[6] However, what happens when the (digital) realities you escape to are controlled and managed by the very same all-powerful evils that've already fucked up the "real" "reality" that you are so eager to escape from? What happens when your very interest or passion for A Thing, be it video games or technology or cyberfeminism, suddenly makes you a target for racialized, ableist, and transmisogynistic digital violence, simply by virtue of you inhabiting a non-normative, devalued, and dispossessed corporeal body in "real life"? *WHY DOES THE SQUISHY FLESH SUIT THAT I HAUNT TEMPORARILY EVEN FRIGGIN' MATTER*?

One would think that in our allegedly fast-approaching technological utopian future,[7] whatever fleshy bits you might happen to have would be irrelevant to your digital

---

[6] Digital escapism was also especially important to me, personally, for gender/bodily dysphoria Reasons, though I certainly don't think one needs to experience dysphoria to appreciate a brief respite from the "real world."

[7] New media studies theorist Martin Lister critiques dominant discourses surrounding our contemporary technological landscape that allude to a digitally enabled social equality, one that "assume[s] that we all have equal access, skill and time; [where] 'the user' becomes a subject category that all too easily transcends material context"; see Martin Lister, et al., *New Media: A Critical Introduction,* Routledge, 2008, p. 207.

experience.[8] Have a dick? No? Two, you say? Doesn't matter! Regardless of the current status of your genitals, you can still access wifi, you can get your 4Gs (areas of coverage notwithstanding, terms and conditions apply, see site for unintelligible details), and you can still check your email and update your Insta and shitpost on Reddit. What your body looks like, feels like, acts like—none of it should have any bearing on how Google lets you google, how Twitter lets you tweet, how tumblr lets you tumbl. One would think.

One would also, unfortunately, be wrong.

There is a false dichotomous conception of digital reality versus IRL reality. Dyadic thinking such as this is harmful to individuals and communities most vulnerable, excluded, and not considered in the development and structuring of the digital spaces. In chapter one I discussed how social media, communication, and information technology corporations structure digital devices, services, and spaces around the extraction of user labor, thereby refiguring users' identities and practices of identity production into monetizable data and users into prosumer subjects. Chapter two explored the serendipitous and covert entanglements between corporate technology companies and U.S. government surveillance, an institutionalized "military-cyberinformation security-technoindustrial complex" that produces and regulates neoliberal docile digital subjects, criminalizing nonideal others (often non-traditionally gendered and/or people of color, especially those associated with or stereotyped as associating with Islam or even

[8] Lol I wish.

appearing vaguely Middle Eastern in descent), domestically and internationally, online and off. In this final chapter I will explore our contemporary digital landscape, looking at the ways in which information and communication technologies and spaces have come to affect and shape us into everyday cyborg subjects, and illustrate how Actually, The Internet is Real Life, and question how we as queer, abject, and subaltern cyborgs might resist cybercapitalist brainwashing, refigure our relationships to technology and to each other, and recreate our own queer digital realities.

Gotta Catch 'em All!

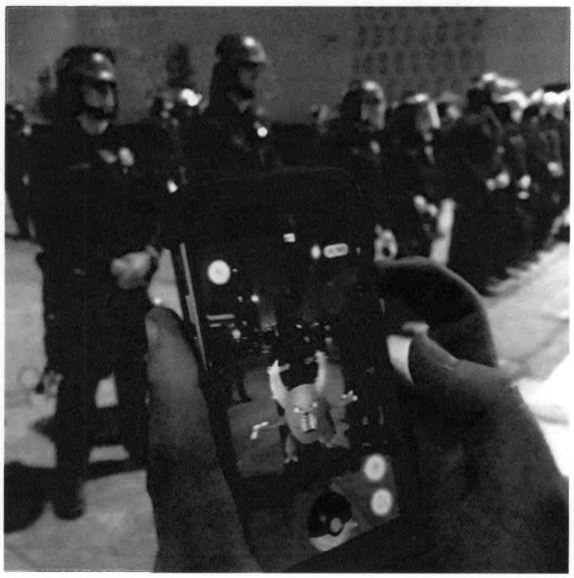


Figure 1: Police officers in riot gear blocking the street in response to a #BlackLivesMatter protest are displayed through the *Pokémon GO* application's "augmented reality" camera lens, and comprise the surrounding background where a Pokémon trainer, presumably a protester, discovers and prepares to catch the Pokémon Pinsir.[9]

[9] Image by @_EricHu, "This week in a single photograph," 9 July 2016, https://twitter.com/_EricHu/status/751915801750495232.

On Tuesday July 5, 2016 in Baton Rouge, Louisiana, Alton Sterling was shot several times point-blank in the chest while pinned to the ground,[10] adding yet another data point to the troublingly frequent cases of trigger-happy law enforcement officers murdering black citizens across the nation with impunity.[11] The very next day in Falcon Heights, Minnesota, Philando Castile was shot four times in the chest during a presumably routine traffic stop in the presence of his four-year-old daughter and her mother, Diamond Reynolds, who live-streamed the murder on Facebook.[12] The video was quickly removed by Facebook, and then later reinstated after user outcry. Facebook explained away their action as a "technical glitch"[13] (I call bullshit). By the end of the week, over 160 Black Lives Matter protesters were arrested in Baton Rouge, a law enforcement response described by Louisiana Governor John Bel Edwards as "moderate," despite the demonstrators' entirely peaceful and non-violent behavior.[14]

---

[10] Abigail Hauslohner and Ashley Cusick, "Alton Sterling's relatives weather scrutiny, call for justice," *The Washington Post,* 13 July 2016, https://www.washingtonpost.com/national/alton-sterlings-relatives-weather-scrutiny-call-for-justice/2016/07/13/dbf0ba60-490f-11e6-bdb9-701687974517_story.html.

[11] *The Guardian* estimates that as of December 1, 2016, 2,114 people have been killed by U.S. law enforcement since the start of 2015; see "The Counted," *The Guardian*, accessed 1 December 2016, https://www.theguardian.com/us-news/ng-interactive/2015/jun/01/about-the-counted.

[12] Andrea Peterson, "Why the Philando Castile police-shooting video disappeared from Facebook—then came back," *The Washington Post,* 7 July 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/07/07/why-facebook-took-down-the-philando-castile-shooting-video-then-put-it-back-up.

[13] Ibid.

[14] Hauslohner and Cusick, "Alton Sterling."

Meanwhile, against this backdrop of public outrage, protests, and anti-police brutality grassroots organizing, emerged a game-changing mobile application that took the nation's attention, money, and hearts by storm.

Pokémon GO is a massively multiplayer online (MMO) mobile augmented reality game (ARG) where players can discover, catch, train, and battle adorable digital creatures (Pokémon), on iOS and Android devices. With over 500 million users worldwide,[15] *Pokémon GO* heralds a new era of location-based gaming, where players are encouraged to physically roam their neighborhoods in search of wild Pokémon and visit real-life public landmarks marked as "Pokéstops" and "Pokémon Gyms" to collect in-game items and gain experience points. *Pokémon GO*'s publisher, Niantic Inc., originally a Google internal software startup founded in 2010, uses the skeleton of its previous location-based ARG from 2012, *Ingress*, as the structural base for Nintendo's incredibly popular Pokémon franchise. Both *Pokémon GO* and *Ingress* use Google Maps' application program interface (API) and Google's user account database as the bones of their software.

The game, which requires either a Google or Club Nintendo account to play, involves designing a "Pokémon trainer" avatar that moves around a digital map based on IRL geography. When a trainer encounters a Pokémon, the game uses the player's mobile

---

[15] Sarah Perez, "Pokémon GO becomes the fastest game to ever hit $500 million in revenue," *TechCrunch*, 8 September 2016, https://techcrunch.com/2016/09/08/pokemon-go-becomes-the-fastest-game-to-ever-hit-500-million-in-revenue.

device's camera and gyroscope to display the creature against a backdrop of the real world, as though the Pokémon was actually standing, flying, swimming, or floating right there in front of you (thus the "augmented" descriptor of this "reality game"). Despite the game's overwhelmingly successful release[16] and widespread acclaim for not only reviving a beloved 90s franchise,[17] but also for bringing hordes of kids (and previously non- gamers) together in the streets to play a game with an emphasis on physical fitness, Pokémon GO's frequent server crashes, bugs, and technical problems (some of which persist to this day) were the subject of much criticism, especially in the earlier days of its release:

---

[16] Nintendo's market value increased by over nine billion dollars within the first week of the game's U.S. release, and within two weeks Nintendo's stock price doubled; "Nintendo market value doubles on Pokémon GO mania," *The Guardian*, 19 July 2016, https://www.theguardian.com/technology/2016/jul/19/nintendo-market-value-doubles-on-pokemon-go-mania.

[17] "Pokémon was never dead!" you might say, but would I argue that to the older generation of us OG 151 Pokémasters, Pokémon as a concept became unrecognizable when Nintendo flipped its wig after *Pokémon Yellow Version* (1998) and decided there were *hundreds more undiscovered Pokémon in the Pokéworld to catch*, making it that much harder to *catch them all.*

Figure 2: A popular meme circulated following the U.S. release of *Pokémon GO* compares Niantic's servers to potato-powered batteries, expressing users' dissatisfaction with the incredibly buggy early versions of the game.[18]

Okay, so perhaps I am willing to entertain the idea that there is no connection between the release of *Pokémon GO* and the nationwide #BlackLivesMatter demonstrations' reignited outrage about the police murders of Sterling and Castile. Perhaps there is no actual link between the sudden, completely unannounced,[19] seemingly unplanned[20]

---

[18] "Pokémon GO Servers" from *Know Your Meme*, submitted by user C_Mill24, August 2016, http://knowyourmeme.com/photos/1144991-pokemon-go.

[19] *Pokémon GO* released a trailer for their game on September 9, 2015, but never announced the game's release date—if they did, I would have friggin' known about it; The Official Pokémon Channel, "Discover Pokémon in the Real World with Pokémon GO!," 9 September 2015, https://www.youtube.com/watch?v=2sj2iQyBTQs.

[20] Prior to its release, a beta version of *Pokémon GO* was only available between to a limited number of players in Japan two short months of testing. After its U.S. introduction, international release dates were postponed due to overloaded server issues; Allegra Frank, "Pokémon GO heading out to the field in Japanese-only beta test," *Polygon*, 4 March 2016, http://www.polygon.com/2016/3/4/11161010/pokemon-go-field-test-beta-japan; and Matt Weinberger, "'Pokémon Go' international rollout will be 'paused' as players overload the system," *Business Insider*, 8 July 2016, http://www.businessinsider.com/pokemon-go-international-rollout-paused-2016-7.

release of a mobile video game that tracks players' locations, peers through their phone cameras, and influences where they congregate and what they do, and the very weekend that thousands of protesters were expected to flock to the streets to voice their condemnation of the government-funded, unindicted police brutality and domestic terrorism against black lives and communities. Perhaps. Or perhaps the most popular and corporate-surveillance-state's-wet-dream of a game was given the green light by the Apple App Store and the Google Play Store to be spontaneously released early in the United States to distract the youths from their nation's ongoing race war. The location-based tracking (and real-time AR camera-snooping) feature,[21] plus the millions upon millions of dollars in micropayment profits, are just delicious manipulative cherries on top. Those pesky millennials are way more manageable when they're in the streets tossing fictional balls at fictional monsters than when they are organizing in resistance against unjust, racially motivated police violence.

---

[21] Another reason I am super convinced that users' movements are being tracked in real-time is the requirement to *have the Pokémon GO app not only running, but open as the primary application on your device for it to count as "playing."* Nintendo as a company is not unfamiliar with movement-based gaming—the "Pokéwalker" was a pedometer designed like a Pokéball introduced in Pokémon HeartGold and SoulSilver that encouraged players to walk around in order to gain experience points to level up their Pokémon. *Pokémon GO* could very easily draw from users' devices built-in pedometers to track walking and distance, but that would mean that the app would not be able to track its users' locations and mine data from their behaviors (such as where they live, what businesses and public spaces they frequent, who they are around, and how they spend their time). If you keep the app open but running in the background, when you return to it (as of its latest release), your avatar's location will jump across the map and the game will issue a "You're going too fast!" alert as though you were driving a car or teleporting across the world. P.S. This annoying and shitty warning is just legal BS to cover Niantic, Apple, Nintendo, and Google's asses when users get into car accidents from pokéhunting while driving.

Maybe this isn't all a huge conspiracy. It is, however, indicative of our contemporary digital era in which corporate technology and social media deities put up consumer-facing fronts, where we the users have little recourse and few options except to blindly trust in corporate entities to prioritize consumers' interests, safety, and security over page counts and profit margins. In a time when brands have personalities and personhood and people have personal brands, where consumers' digital footprints are constantly monitored "to improve user experience" and service providers still pretend that there is any alternative response to a terms and services agreement other than "I accept," how could we possibly buy the story that users mean anything more than data points and dollar bills?[22]

Since the police killings of Eric Garner, Michael Brown, and Treyvon Martin over two years ago the public is becoming increasingly aware of incidents of police brutality against black Americans, thanks to the growing prevalence of social media and access to communication technologies. I am not saying that there are increasing rates of black people murdered by law enforcement officials, because they may be just as much as before—in fact, there still fails to exist any government accountability or statistics on the number of black people murdered by police domestically. Presently, the FBI only

[22] I recently dated a woman who previously worked for Facebook and was part of developing an internal company- wide initiative to refer to Facebook users not as "users" but as "friends." She also tried to convince me that Facebook was "really about connecting people" and not about making billions of datamining dollars off the backs of prosumer user labor. I asked why Facebook was so concerned with tracking my every move, both on and off the site, she assured me that "oh no, you're just a number to us." I'm not sure what they put in the contradictory bullshit kool-aid they serve on Facebook's campus, nor if my recounting of our conversation here counts as noteworthy academic research, so maybe just consider this a fun anecdote.

maintains records on "justifiable homicides," which are *voluntarily* reported by state and local law enforcement agencies and generate widely inaccurate numbers,[23] reflecting the U.S. government's willful obfuscation of and complicity with government resources used to kill people of color. Racially motivated police violence has only made its way into the recent widespread social consciousness thanks to instantaneous social media-enabled, user-generated digital sharing. Social media and digital technologies can be effective tools for #BlackLivesMatter and other grassroots activist organizing.[24] At the same time however, social media platforms also present challenges unique to digital spaces because the ruling corporate overlords DGAF.

I would like to be excluded from this narrative, kthx

My previous chapters illustrated several ways that we can recognize power in and over digital spaces. We can witness how social media companies like Facebook and Google structure their services and platforms around maximizing valuable data extraction and participate in corporate networks of market data trading, all at the expense of consumer privacy and through the exploitation of digital user labor. Furthermore, the very same technological superpowers that create and control our means of

[23] *The Guardian* has described the current civilian fatality accounting system as "arguably less valuable than having no system at all," which inspired the project, "The Counted"—a verified, crowdsourced database of people killed by police and law enforcement agencies in the United States since 2015; see "The Counted," *The Guardian*, https://www.theguardian.com/us-news/ng-interactive/2015/jun/01/about-the-counted.

[24] In an August 2016 report for the Pew Research Center, the hashtag #BlackLivesMatter was found to be one of the most influential hashtags in the history of Twitter, and is predominantly used for the purposes of social organizing and expressing race-related social unrest; see Monica Anderson and Paul Hitlin, "Social Media Conversations About Race," *Pew Research Center*, 15 August 2016, http://www.pewinternet.org/2016/08/15/social-media-conversations-about-race.

communication designate themselves the arbiters of privacy and security, feigning compassion and acting the protectors of consumer interests, while simultaneously allowing government institutions access to an unbridled arsenal of surveillance resources. This ever-present surveillant assemblage haunting our digital realities in the name of "national security" not only polices our behaviors online, but further seeps into regulating real-life subjects, bodies, and embodiments, which I will soon demonstrate through a deeper examination of #BlackLivesMatter. Where does this leave non-normative and non-ideal digital subjects navigating online spaces not made for them, where their intelligibility is limited by dominant knowledge frameworks grounded in neoliberal and nationalist capitalism?

Joan W. Scott deconstructs dominant processes of knowledge production in her 1991 piece, "The Evidence of Experience," which can help illuminate the ways in which our understandings of "authoritative" knowledge and power work to shape and delimit our possible conceptions of "truth" and "reality." Furthermore, through a critique of visibility and the "visible," Scott offers potential strategies with which we might analyze and challenge hegemonic constructions of reality, and expand our capacity for recognizing alternative knowledges and subject positions. She first draws upon Samuel R. Delany's *The Motion of Light in Water* and his attempt to render visible and construct a deviant historical narrative of homosexuality, thereby challenging hegemonic heteronormative histories and exposing the ways in which they naturalize their construction through the exclusion of histories of difference. Scott argues that by making

his experience of difference visible through his written account, and using that experience as evidence of a broader "truth" that contests and expands upon dominant knowledges, Delany's articulation of homosexual visibility can only be understood within the preexisting ideological system by which categories of representation are understood; that is, as a difference relationally constituted against the category of heterosexual identity.[25] Although the newly-rendered visibility of the homosexual category poses an alternative critique of existing norms that highlights the socially instituted repression of homosexual identity, Scott argues that the evidence of lived experience in Delany's project functions to reproduce and supplement the ideological framework by which difference is read, without questioning the greater sociohistorical system by which subjects of difference are constituted as such:

> We know [nonnormative subjects] exist, but not how they have been constructed; we know their existence offers a critique of normative practices, but not the extent of the critique. Making visible the experience of a different group exposes the existence of repressive mechanisms, but not their inner workings or logics; we know that difference exists, but we don't know how it is relationally constituted. For that we need to attend to the historical processes that, through discourse, position subjects and produce their experiences. It is not individuals who have experience, but subjects who are constituted through experience.[26]

---

[25] Joan W. Scott, "The Evidence of Experience," *Critical Inquiry* vol. 17, no. 4, University of Chicago Press (1991): 773-797, p. 778.

[26] Ibid., p. 779.

Scott argues that historians and knowledge producers must attend to the ways in which the constructed nature of experience and visibility are shaped by historical and discursive processes that position subjects within a preexisting framework of intelligibility. Using a subject's personal experience as evidence of an authentic representation of reality "establishes the prior existence of individuals," and assumes a prediscursive truth about categories of difference that recognizes the individual as the primary source of knowledge without recognizing the ways in which the subject's conception of self and their understanding of experience is already mediated through discursive operations of power.[27] In effect, "experience" as evidence "naturalizes categories such as man, woman, black, white, heterosexual, and homosexual by treating them as given characteristics of individuals," and functions to ahistoricize and essentialize such categories of difference according to the ideological system that predefines the terms of visibility and intelligibility as relationally constituted.[28]

At this crucial stage in our technological history, where new questions of digital privacy, state and corporate surveillance, and data ownership hang in the balance, it is imperative that we question how the conditions of visibility and intelligibility in digital spaces are centered around and limited by the imperative to measure and evaluate users and user data in terms of capital. Digital expressions of difference, then, can only be read through lenses established and upheld by the institutionalized hegemony that control

[27] Scott, "The Evidence of Experience," p. 782.

[28] Ibid.

what is and is not visible online, and what visibility even looks like in online spaces. Furthermore, in the case of the tech industry, the primacy, valuation, and trust given over to the alleged "objectivity" of computer algorithms to recognize patterns of user characteristics and behaviors and make inferences recognized as legitimate truth absent of human error—because *science*—is a fraught discursive strategy that ignores the preexisting ideological assumptions that inform the knowledge from which programs are programmed, and computers are taught to compute.

The cost of "becoming visible" in Scott's argument is the essentialization of different identity categories in order to conform to the preexisting framework of hegemonic knowledge. This phenomenon is illustrated in Evelynn Hammonds' article, "Black (W)holes and the Geometry of Black Female Sexuality," in which she argues that the intelligibility of black female sexuality as read within dominant frameworks of knowledge is simultaneously invisiblized and hypervisible when oppositionally defined against white female sexuality. She writes: "Black women's sexuality is often described in metaphors of speechlessness, space, or vision, as a 'void' or empty space that is simultaneously ever visible (exposed) and invisible and where black women's bodies are always already colonized."[29] In her construction of a historical genealogy of the dominant discursive representations of black female sexuality as absent, Hammonds argues that hegemonic knowledges "colonize" the black female body through processes of erasure,

[29] Evelyn Hammonds, "Black (W)holes and the Geometry of Black Female Sexuality," *differences* 6: 2+3, Indiana University Press (1995): 126-146, p. 383.

forced silence, and pathologization in order to oppositionally produce notions of ideal white female sexuality. Much like Delany's representation of a homosexual identity constituted relationally to the more visible heterosexual identity category, the attempts to theorize a racialized sexual difference of black female sexuality within the terms by which white female sexuality is understood produces a flattening effect that reduces conceptions of black female sexuality to the negative stereotypes of immorality and hypersexuality. In effect, such essentialization denies the black female subject complexity—she is hypervisible, represented as deviant sexuality, yet also invisible within an ideological system that pre-emptively defines her and leaves her with no means of self-articulation.[30]

Hammonds problematizes visibility and the ways in which visibility informs hegemonic knowledges by using the metaphor of black female sexuality as a "black hole." In the field of astrophysics, the existence of black holes is detectable only through their distorting effects on "normal" visible stars in the surrounding area. Generally, to the outside observer, one conceives of black holes as empty voids in space, when in reality they are comprised of an immense density with a gravitational influence on the space around it. Following this metaphor, if black female sexuality can be represented as a "black hole" detectable only through its distorting influence when read against the "normal" visible star that is white female sexuality, then the dense complexity of black

[30] Hammonds, "Black (W)holes," p. 384-385.

female sexuality cannot be fully detected nor realized within the knowledge framework that enables the visibility of white female sexuality.[31]

Scott echoes Hammonds' concerns regarding the attendant epistemological oversight and negligence when our notion of the "visible" is prediscursively assumed and afforded uncritical primacy in the production of knowledge. She writes,

> Knowledge is gained through vision; vision is a direct apprehension of a world of transparent objects. In this conceptualization, the visible is privileged; writing is then put at its service. Seeing is the origin of knowing. Writing is reproduction, transmission—the communication of knowledge gained through (visual, visceral) experience.[32]

The production of hegemonic knowledge is predicated upon that which can be read as visible, which is then translated through the experience of that vision and reproduced in language, which is already pre-inscribed with meaning. The world therefore does not consist of "transparent objects" that can be represented in some form of pure "truthful" knowledge; rather, discursive power operates in ways that privileges certain objects over others by structuring the conditions of visibility. Black female sexuality can never be fully represented or made knowable within the limited conditions that privilege and make visible normative white female sexuality—within the existing terms that structure knowledge; it will only ever be read as pathologized absence and

---

[31] Hammonds, "Black (W)holes," p. 388.

[32] Scott, "The Evidence of Experience," p. 775-776.

silence. How then can we remedy these constructed absences within the domains of hegemonic knowledge in order to fully recognize a complex black female subjectivity and, further, enable the theorization of different nonnormative subjectivities?

Hammonds argues that "we need to develop reading strategies that allow us to make visible the distorting and productive effects these sexualities produce in relation to more visible sexualities."[33] Once we can recognize the socially and historically instituted dynamics of power that replicate and reinforce the structure of knowledge production, experience, and visibility in the service of reproducing hegemonic normativity, we can begin to theorize different ways of restructuring the terms of legibility in order to recognize black female subjectivity. Hammonds suggests an alternative geometry resistant to the essentializing functions of hegemonic knowledge, one that centers the black female subject and explores a nuanced "politics of articulation" that critically interrogates the intricacies of power and domination that structure what counts as authentic knowledge and what types of knowledge are foreclosed upon.[34] Breaking away from hegemonic processes of knowledge production and the discursive systems that sustain it can, in the greater sense, help us to articulate alternative conceptions of what counts as knowledge, re-evaluate experience and visibility as historically and socially constituted, recognize the ways in which certain knowledges are produced at the expense

[33] Hammonds, "Black (W)holes," p. 388.

[34] Ibid., p. 390.

of subaltern or nonideal subjects, and create the potential to change the conditions of possibility that limit our understandings of reality.

The Cake is a Lie

Before I begin to explore what this "alternative geometry" might look like in digital spaces, one that might allow for a "politics of articulation" of differently situated digital subjectivities, I want to quickly return to two specific cases from #BlackLivesMatter and #GamerGate to demonstrate the real-life, lived consequential violence of hegemonic conditions of digital (in)visibility and its attendant epistemological "black holes" around black and people of color users' digital subjectivities.

Following the deaths of Alton Sterling and Philando Castile at the hands of law enforcement, five police officers were killed and seven injured during a #BlackLivesMatter protest in Dallas, Texas. Although the protesters were reportedly peaceful,[35] it did not stop the Dallas Police Department (@DallasPD) from immediately tweeting a photograph of #BlackLivesMatter organizer Mark Hughes, identifying him as a key suspect:

---

[35] Joel Achenbach, William Wan, Mark Berman, and Moriah Balingit, "Five Dallas police officers were killed by a lone attacker, authorities say," *The Washington Post,* 8 July 2016, https://www.washingtonpost.com/news/morning-mix/wp/2016/07/08/like-a-little-war-snipers-shoot-11-police-officers-during-dallas-protest-march-killing-five.

Figure 3: @DallasPD's tweet identifying #BlackLivesMatter protest organizer Mark Hughes as a murder suspect and calling upon the twitter public for help is retweeted over 38 thousand times. The original tweet has since been deleted (screenshot is my own).

@DallasPD's accusatory tweet was quickly met with conflicting evidence of Hughes' alibi tweeted by a number of #BlackLivesMatter witnesses present at the protest.[36] Despite clear evidence of its falsehood, @DallasPD failed to delete their slanderous tweet for over 24 hours, and its overwhelming number of retweets guarantee its misinformation permanent residence in the digital imaginary. It did not take long for #Dallas #BlackLivesMatter and the newer "#bluelivesmatter"[37] hashtags to blow up with extremely racist threats of violence against Hughes and other protesting "rioters" considered "domestic terrorists" by Twitter's resident white supremacists.[38] @DallasPD did eventually tweet an update that "The person of interest whose picture has been circulated just turned himself in,"[39] however they failed to ever recognize his innocence, issue an apology, or acknowledge their racially-motivated and stereotypical criminalizing misrepresentation of a black man who was protesting law enforcement's violent misuse of excessive force against people of color. Instead, the Dallas Police Department opted to

---

[36] Users including @nhlmurphy, @dallasnewsphoto, and @YahBoyEric tweeted photos and videos confirming that Mark Hughes was peacefully protesting at the time of the shooting; @nhlmurphy, "@DallasPD but y'all know you have the wrong suspect, right?" 7 July 2016, https://twitter.com/nhlmurphy/status/751271612637257729; @dallasnewsphoto, "Shots fired at #blacklivesmattertx march," 7 July 2016, https://twitter.com/dallasnewsphoto/status/751235966505881600; @YahBoyEric, "@DallasPD he is on the floor doing nothing come on now," 7 July 2016, https://twitter.com/YahBoyEric/status/751271645742977024.

[37] The hashtag #bluelivesmatter emerged in response to #BlackLivesMatter as a reactionary movement in defense of police and law enforcement officials. Much like the similarly offensive and racist hashtag #alllivesmater, #bluelivesmatter attempts to criminalize and diminish the legitimate concerns of black communities disproportionately targeted by police brutality.

[38] In interest in not implicating myself in the circulation of this particular brand of vitriolic digital hatred, I will not be citing any of these awful tweets. However, far too many can be found in the threaded responses to @DallasPD's tweet cited in the following footnote.

[39] @DallasPD, "Update," 7 July 2016, https://twitter.com/DallasPD/status/751271541459984384.

continue alluding to Hughes' alleged involvement and perpetuate the same, business-as-usual racist ideologies that got us here in the first place. Thanks to the authority of less than 140 Twitter-verified characters, the person running the @DallasPD Twitter account drew a digital target on Mark Hughes' back and likely ensured his life would never be the same again.

Veerender Jubbal (@veeran_jubbal) was similarly made a victim of racially-motivated information manipulation. Creator of #stopGamerGate2014,[40] a movement against one of the most notorious troll hordes in the history of the internets, Jubbal was no stranger to cyberharassment, especially as a practicing Skih and self-proclaimed "Social Justice Healer." That was, however, until the November 2015 Paris attacks, when a group of #GamerGaters circulated a photoshopped image of Jubbal in a bomb vest, falsely accusing him of being a suicide bomber:

[40] @veeren_jubbal, "#StopGamerGate2014," 14 October 2014. https://twitter.com/Veeren_Jubbal/status/522185406263988224.

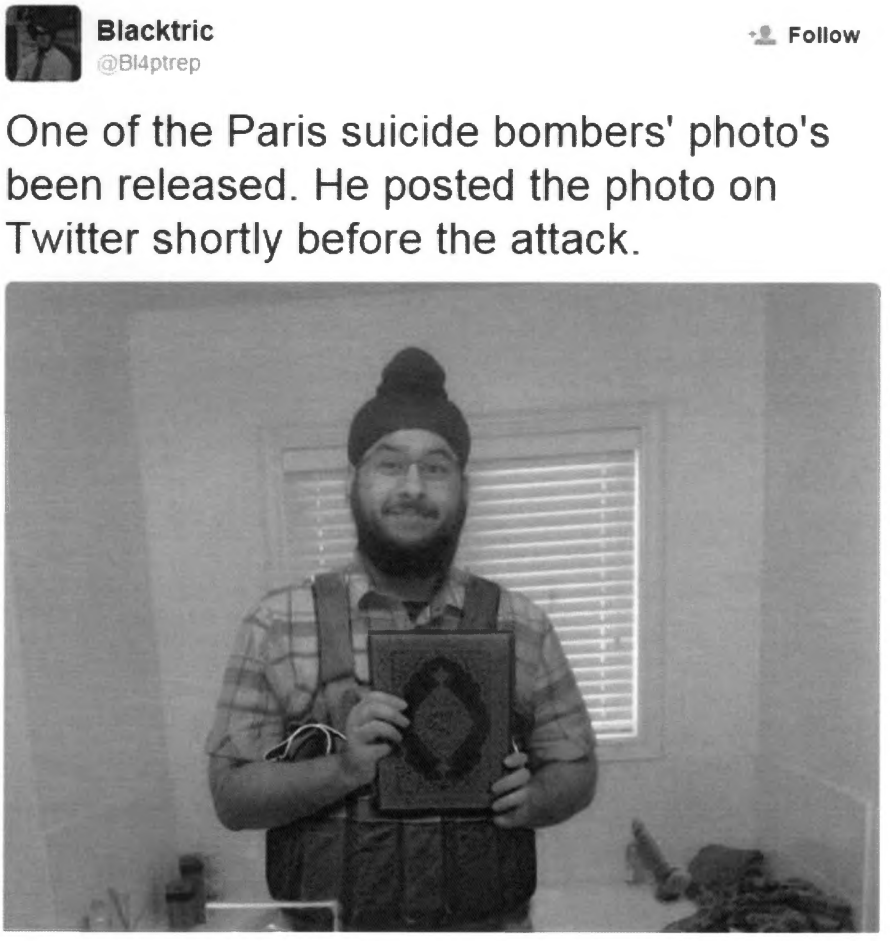


Figure 4: @Bl4ptrep's original tweet featuring a photoshopped Jubbal attracted the attention of numerous international news media outlets, demonstrating the dangers of viral internet misinformation combined with Islamophobia and anti-feminist sentiment.[41]

[41] @Bl4ptrep's Twitter account has been deleted, but the Tweet remains available on the internet archive. 14 November 2016, https://web.archive.org/web/20151114003205/https:/twitter.com/bl4ptrep/status/665323528279855104.

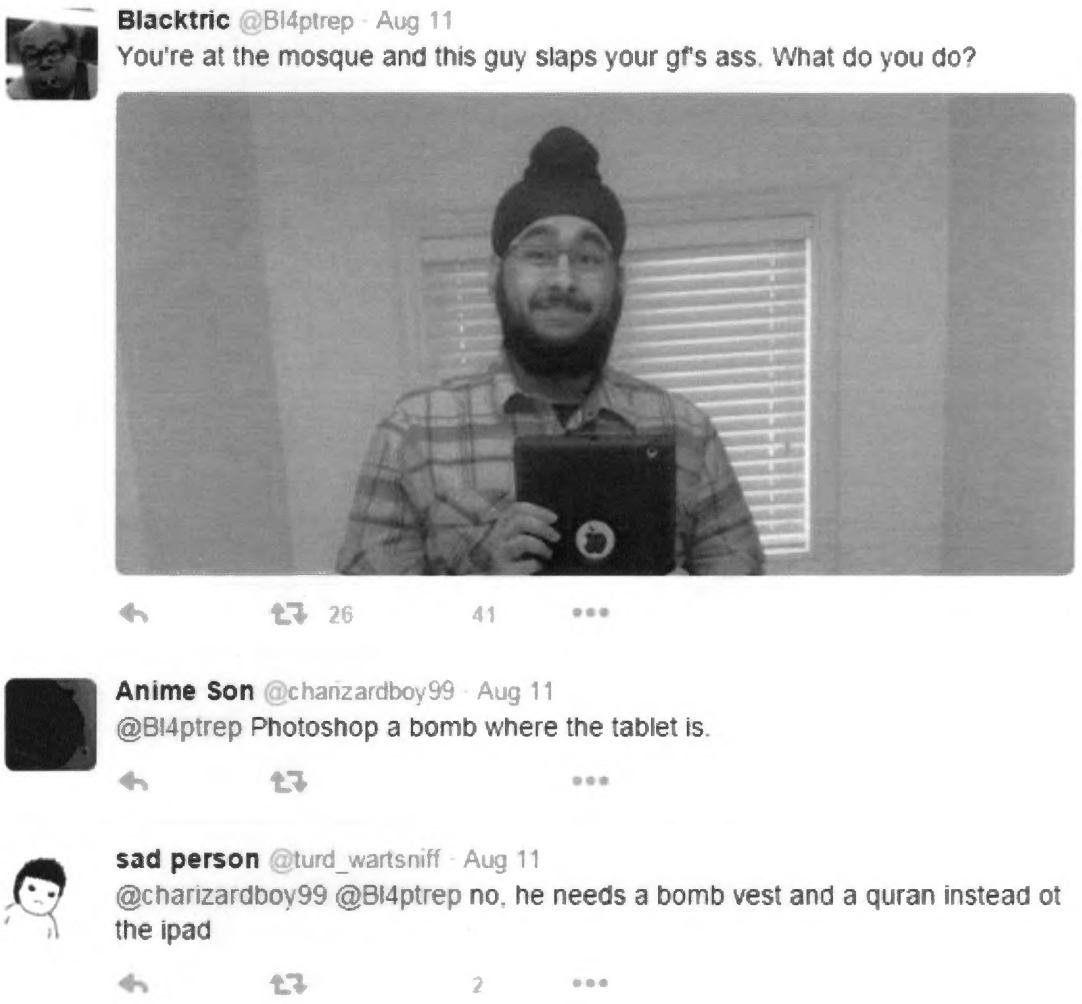


Figure 5: Twitter users @Bl4ptrep, @chariszardboy99, and @turd_wartsniff showcase their casual internet racism. *Vice* reporter Rich Stanton's internet detectiving tracked the users back to r/KotakuInAction, the Reddit headquarters of #GamerGate.[42]

[42] Rich Stanton, "GamerGate Members Are Responsible for the Terrorist Photograph of Journalist Veerender Jubbal," *Vice*, 17 November 2015, http://www.vice.com/en_uk/read/gamergate-members-are-responsible-for-the-terrorist-photograph-of-journalist-veerender-jubbal-503.

The photoshopped image of Jubbal went viral and was quickly disseminated across international news outlets. Once a prolific member of Twitter, with over twelve thousand followers and nearly fifty thousand tweets, @veeran_jubbal has not tweeted since December 2015.

Mark Hughes and Veerender Jubbal's experiences demonstrate how rampant viral misinformation catalyzed by racist ideologies work to disseminate digital cultural discourses and construct digital realities that have virtual and real-life consequences for vulnerable users of color. At any point, Twitter could have stepped up and put a halt to the malicious spread of information, rather than sit back and watch its service provide a digital platform for naturalizing the criminalization of people of color and rationalizing their surveillance. Instead, it has become commonplace for tech behemoths like Twitter and Facebook to act as complicit extensions of the U.S. state; censoring the violent realities of racially-motivated police brutality[43] and supporting law enforcement's racial profiling by providing facial recognition software and social media data to aid in the arrests of #BlackLivesMatter protesters.[44]

My goal here was to construct a brief genealogical illustration of contemporary operations of power and authority on the internet, and to demonstrate their effects on

---

[43] I am referring to Facebook's decision to block Diamond Reynold's video of Philando Castile's murder, which I discussed earlier in the chapter.

[44] Sidney Fussell, "How Facebook, Instagram, and Twitter helped police target black activists," *Fusion,* 12 October 2016, http://fusion.net/story/356808/facebook-twitter-instagram-geofeedia-tracking.

shaping digital spaces, sociality, and subjects. We can see how institutionalized state and corporate powers work together to construct and uphold hegemonic digital spaces and realities that not only enable, but also catalyze cyberviolence against abject and subaltern subjects. When tech corporations only recognize digital subjects in dollar valuations and the government only recognizes digital subjects as docile patriots or suspicious terrorists and criminals, when our digital and physical safety is no guarantee in the virtual wild west, when we see our humanity, identities, and selves reduced to a collection of ones and zeroes, it's no wonder we have come to build and believe in a cognitive barrier between our digital and real realities. Such a barrier makes it that much harder to users to recognize that there are *other humans* on the other side of the screen, with other digital experiences and digital realities different from themselves', and with other physically embodied affects as a result. Corporate and state powers deploy this dyadic thinking as a strategy to divide and conquer—as makers of our digital worlds, we leave it up to them to define safety and (cyber)humanism when they designate which subjects comprise the protected class of digital consumer-citizen.

A Digital Politics of Articulation

I argue that, in order for not only subaltern, but also "normative"-ly defined digital user-subjects to begin to resist these limiting epistemological lenses, we need to develop a politics of articulation that is critical of the dehumanizing and necropolitical, racialized and gendered processes of digital subjectification grounded in neoliberalism, capitalism, and nationalism; in order to break beyond the cognitive borders that separate

the "digital" and the "real," and extend the terms of intelligibility and recognition of other subjects as legitimate, valued, and human. My strategy for a digital politics of articulation draws inspiration from queer and feminist theoretical frameworks by Judith Butler and Karen Tongson. I write with the caveat that I recognize I cannot articulate a fully-comprehensive, end-all-be-all strategy to Fix The Internet—I know I cannot overthrow capitalism with a single tweet, unfortunately, no matter how hard I try—but I do want to use whatever mystical powers I have in writing a MA thesis to introduce into the academic discourse the incredible overlap between queer and feminist concerns with identity and subjectivity, and our incredibly complex relationships to digital technologies and spaces. It is my hope to highlight and inspire future discussions about the transformative potential for queer and feminist epistemologies to positively change digital sociality.

The first part of my strategy for a digital politics of articulation is grounded in Judith Butler's notion of humanism, which she establishes in the essay "Violence, Mourning, Politics." Butler argues for a concept of humanism based on mutual recognition of shared a corporeal vulnerability.[45] She questions how we as feminists might ethically conceptualize the often fractured and multiple subject positions that inhabit the literal and discursive spaces where non-normative, abject, and otherwise subaltern subjects are rendered unintelligible as whole and complete subjects, but rather

[45] Judith Butler, "Violence, Mourning, Politics," *Precarious Life: The Powers of Mourning and Violence,* Verso: 2004, p. 19-49: p. 42-43.

are reduced to the ideological "other" against which normative subjects are relationally constituted.[46] Butler argues that the first step toward expanding the terms of recognition and intelligibility, and thereby opening up the potential for realizing multiple and situated subjectivities as contextually and relationally constituted, is by acknowledging others as humans, like ourselves, who are capable of suffering harm.[47] In striving for this mutual recognition we can begin to see the relationality behind our own subjectivities, that we are not permanently fixed to a bounded "subject position" but are rather in a constant, changing state of always-becoming in relation to those around us.[48] For subjects in digital spaces, this humanist framework requires that we resist reductive and essentializing conceptions of identity and subjectivity as prediscursive and immutable, and see past the state and corporate discourses that uphold fictive divisions between the digital and real in order to recognize how digital actions have corporeal effects.

This leads into the second part of my strategy; to recognize the vulnerability of another requires recognizing one's own vulnerability, and it is in these moments of shared vulnerability where the potential for transformative social understanding lies. How do we conceptualize this digital recognition, and what might these moments of contact look like? Furthermore, how can we cultivate the potential for positive and nonviolent opportunities to recognize different subjectivities across digital spaces, especially when

---

[46] Butler, "Violence, Mourning, Politics," p. 41.

[47] Ibid., p. 46.

[48] Ibid., p. 46-47.

the conditions of visibility in digital spaces are so often determined by state and corporate powers invested in reinforcing institutionalized neoliberal capitalism? For insight I turn to Karen Tongson's *Relocations: Queer Suburban Imaginaries.*

Tongson uses the concept of a cloverleaf freeway interchange as a spatial metaphor that offers us a way to envision the shifting and discursive co-productive relationship between rural, urban, and suburban spaces and what they represent within dominant ideological spatial imaginaries. Tongson examines several different locations in Southern California and critiques traditional ideological notions of the suburbs as representing the white heteropatriarchal capitalist American dream, when in reality such spaces and dreams are reliant upon the labor of low-income, blue collar, and service working class communities of color excluded from the suburban imaginary narrative. She cites numerous examples of queer approaches to capitalist consumption practices to demonstrate how the suburbs, the ideological site of normativity, in reality includes covert expressions of queer subjectivity that resist and contradict the assumed and intended subjectivizing operations of imperial capitalism. Tongson proposes that these non-ideal queer and subaltern subjects, those that discreetly occupy the many suburban hypercapitalist "nowheresvilles" not made or intended for them, yet inhabit them nonetheless, can carve out survival strategies and community by refiguring their relationships to capitalist consumption. Tongson names these strategies "remote intimacies," which describe the shared identificatory affiliations with inhabiting the various nowheresvilles across time and space, existing contrary to hegemonic

epistemologies that claim otherwise and hinting at the possibility of destabilizing normativity.[49]

Applied to digital spaces, we can conceptualize "remote intimacies" as the multiplicity of digital worlds and realities algorithmically constructed, curated, and specifically personalized for individual users; digital worlds and realities intended for ideal digital subjects, yet occupied, reconfigured, and navigated by non-ideal "others." Cultivating "remote intimacies" across Facebook newsfeeds, Twitter timelines, and Tumblr dashboards—that is, finding a shared (lack of) belonging within the overlapping network of digital realities built around maximizing corporate profit—reveals the fallibility of digital normativity and subject production. Returning to Tongson's cloverleaf spatial metaphor, we can envision the multiplicity of our different digital experiences as a complex, social choreography of traffic interchange on the information superhighway. Tongson writes:

> Cloverleaf interchanges require an elaborate choreography between vehicles and drivers. Rather than merging directly onto the flow of traffic with the aid of lights and signals, the cloverleaf offers an interstitial lane on which vehicles traveling at different speeds and at cross-purposes—some exiting, others entering—negotiate their transactions of motion within a death-defying instant... the dangerous transaction, the elaborate dance between drivers destined for different directions, yet forced by design to notice one another as if their lives depended on it, because they

[49] Karen Tongson, *Relocations: Queer Suburban Imaginaries,* New York University Press: 2011, p. 23.

> do in that instant. The suburban and the urban, queer narratives and normative ones, history and theory, may be at cross-purposes and propelled by different velocities toward different destinations, but I force them to interact in *Relocations* as if they were on one of these cloverleaves: they meet transiently, aware they're inhabiting one another's blind spots, and yet they are willing to yield their right of way to take the risk of crossing in time and space together, lest there be a fatal and catastrophic collision.[50]

As users, we drive around in different digital realities, seeing and experiencing our digital worlds as our corporate overlords will allow, each claiming to some extent to represent an accurate, truthful, or universal version of reality. However, once we pull back the veil of institutionalized capitalist extraction and idealistic consumer-subject production, we can begin to spot the in-between digital "elsewheres" and "nowheresvilles" occupied by improper subjects and explore alternative means of digital belonging. It is in these brief, transient moments of contact that mutual recognition might be achieved, where users can cultivate remote intimacies through a shared understanding of situated differences, recognize their co-constitutive relationships, and create the potential to recognize alternate realities, experiences, and knowledges as legitimate and valid.

To close, I offer what I believe to be an emerging digital movement that exemplifies positive, collective "remote intimacies" that promote alternative digital politics that actively work to recognize, validate, value, and radically support subaltern

---

[50] Tongson, *Relocations*, p. 8.

digital subjects. Crash Override Network is a self-proclaimed "anti-online harassment task force" founded and organized by Zoë Quinn as a direct result of her struggle to be taken seriously by law enforcement and social media providers regarding #GamerGate harassment. When met with these authorities' disbelief and blanket disavowal of responsibility, Quinn turned to alternative channels for recourse and support. As a collective of hackers and hacktivists dedicated to creating a network of survivors of cyberviolence, Crash Override's focus is on building a respectful and healing online community, as well as developing public educational resources about online harassment and information security in order to empower users to gain control of their data, spaces, and realities both online and off. Crash Override's activism employs four primary strategies: First, they work to empower targets of cyberviolence by providing practical guides to personal digital security; for instance, their "So You've Been Doxed: A Guide to Best Practices" explains how to document instances of online harassment, when and how to reach out to law enforcement, and methods to scrub private information from online databanks and prevent further doxing attempts.[51] Second, Crash Override practices activism through education by providing resources such as their "Guide for Employers" and "Guide for Talking to Family & Police," intended to help explain cyberviolence and its material effects in accessible terms for people and figures of authority who might not understand technobabble or the potential dangers that women, people of color, queer,

[51] Crash Override Network, "So You've Been Doxed: A Guide to Best Practices," 21 March 2015, http://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices.

transgender, feminist, and otherwise nonnormative people face in online spaces.[52] Thirdly, they implement direct action with on-call crisis center support, which engages a network of hacktivists, information security professionals, and legal experts—most of whom are survivors of cyberviolence themselves—to assist targets of abuse by working immediate damage control, making sure to secure users' sensitive personal information, and exposing perpetrators of digital and real-life violence. Finally, and perhaps most importantly, Crash Override Network facilitates support groups for people experiencing cyberviolence, offering commiseration, counseling, and community. Although their members comprise many differing situated identity locations, what they share in common is the desire to cultivate nonviolent digital spaces where all users are free to explore digital self-expression without fear of reprisal. What we can learn from an organization like Crash Override Network is how coalitional grassroots social movements can circumnavigate the restrictive and oftentimes cyberviolent digital structures, cultures, and boundaries constructed by neoliberal, capitalist, and nationalist imperatives on private corporate and governmental institutions by doing the radical work of recognizing, supporting, and listening to dispossessed and vulnerable digital subjects.

I began this chapter with a discussion of Pokémon GO because I feel that the game represents an easy gateway for users to witness the potential overlap between our

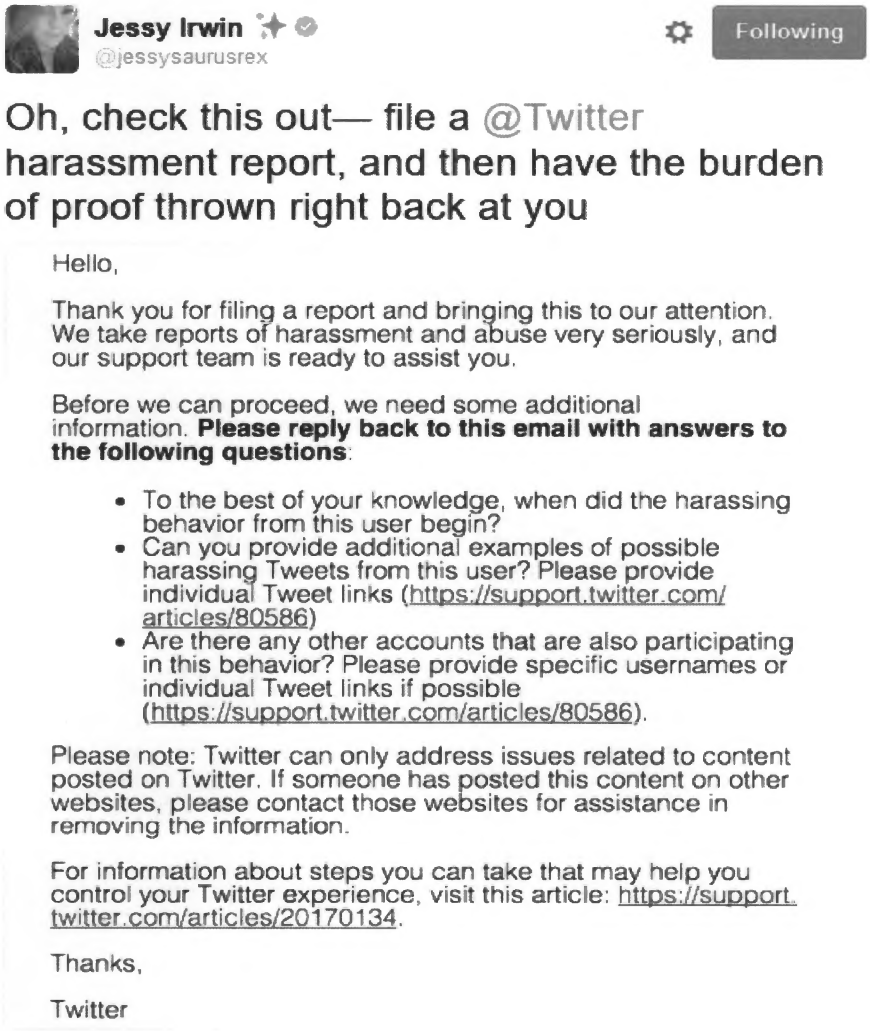
---

[52]Crash Override Network, "Guide for Employers," 27 Apr 2015, http://www.crashoverridenetwork.com/employers/; and "Guide For Talking to Family & Police," 15 Mar 2015, http://crashoverridenetwork.tumblr.com/post/113748237272/guide-talking-to-family-police.

digital and "real" realities. For many users, Pokémon GO is their first exposure to augmented reality, one where digital information is presented as though it inhabits and shares in the user's physical space and reality, thereby transforming their perception of the real world. No longer trapped behind a screen, the invisible Pokémon roaming around us, hidden around the corner just waiting to be caught, can help blur the conceptual boundary between the digital and the real. My argument is that our realities were already augmented, even if the fact wasn't previously made visible by the presence of adorable monsters. Because we might not always see the effects of digital technologies on our lived realities, it is important to question how and why digital spaces and technologies are structured in the way they are, and the epistemological truths and realities they reinforce. We must strive to recognize and render visible the subjectivizing processes of technology on users, with an exceptionally critical eye toward digital authorities' disavowal of and invisiblizing violence against non-ideal and dissenting subjects that fall outside the proper physical and virtual embodiments demanded by neoliberal capitalism. When we, as tech users, consumers, producers, and cyberfeminists, can recognize the phenomenological blind spots within the dominant digital discourses and imaginaries that enable and legitimize necropolitical violence, both online and off, we can begin to reconfigure our relationships with and within different digital spaces and technologies, and explore resistant, humanist, and nonviolent approaches to digital sociality.

Appendix

Figure 1:



InfoSec expert Jessy Irwin exposes Twitter's lacking infrastructure for addressing online harassment, as well the displacement of responsibility onto cyberviolence victims, which inadvertently functions to discourage reporting abuse; @jessysaurusrex, 12 March 2016, https://twitter.com/jessysaurusrex/status/708787029123792898.

Figure 2:

InfoSec expert Jessy Irwin's tweet highlights oversights in social media profile management, particularly for women and other vulnerable users concerned with public and private information. This tweet points not only to privacy issues not addressed on Instagram, but also the oblique nature of social media profile privacy settings that causes Irwin to tweet for help; @jessysaurusrex, 2 October 2016, https://twitter.com/jessysaurusrex/status/782751109064433664.

Figure 3:

"On the Internet, nobody knows you're a dog."

Peter Steiner's 1993 "On the Internet, nobody knows you're a dog" is *The New Yorker*'s most-reprinted illustration of all time.

Bibliography

Achenbach, Joel, William Wan, Mark Berman, and Moriah Balingit. "Five Dallas police officers were killed by a lone attacker, authorities say." *The Washington Post.* 8 July 2016. https://www.washingtonpost.com/news/morning-mix/wp/2016/07/08/like-a-little-war-snipers-shoot-11-police-officers-during-dallas-protest-march-killing-five.

Anderson, Monica and Paul Hitlin. "Social Media Conversations About Race." *Pew Research Center.* 15 August 2016. http://www.pewinternet.org/2016/08/15/social-media-conversations-about-race.

Alexander, Leigh. "But WHAT CAN BE DONE: Dos and Don'ts to Combat Online Sexism." 5 July 2014. http://leighalexander.net/but-what-can-be-done-dos-and-donts-to-combat-online-sexism.

American Civil Liberties Union. "Domestic Drones." Accessed 17 May 2016. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones.

----- "Stingray Tracking Devices: Who's Got Them?" Accessed 17 May 2016. https://www.aclu.org/map/stingray-tracking-devices-whos-got-them.

"APPLE INC'S MOTION TO VACATE ORDER COMPELLING APPLE INC. TO ASSIST AGENTS IN SEARCH, AND OPPOSITION TO GOVERNMENT'S MOTION TO COMPEL ASSISTANCE." United States District Court: Central District of California, Eastern Division. 25 February 2016. https://www.documentcloud.org/documents/2722199-5-15-MJ-00451-SP-USA-v-Black-Lexus-IS300.html.

"Assassin." Newgrounds. http://www.newgrounds.com/collection/assassin.

Balko, Radley. "Surprise! NSA data will soon routinely be used for domestic policing that has nothing to do with terrorism." *The Washington Post.* 10 March 2016. https://www.washingtonpost.com/news/the-watch/wp/2016/03/10/surprise-nsa-data-will-soon-routinely-be-used-for-domestic-policing-that-has-nothing-to-do-with-terrorism.

Beauchamp, Toby. "Artful Concealment and Strategic Visibility: Transgender Bodies and U.S. State Surveillance After 9/11." *Surveillance and Society* 6(4) (2009): 356-366.

Blue, Violet. "Advertising's hottest surveillance software is surprisingly legal." *Engadget*. 25 March 2016. http://www.engadget.com/2016/03/25/advertisings-hottest-surveillance-software-silverpush.

Bogado, Aura. "Native Americans Say Facebook Is Accusing Them of Using Fake Names." *Colorlines*. 9 February 2015. http://colorlines.com/archives/2015/02/native_americans_say_facebook_is_accusing_them_of_using_fake_names.html.

Broadband Commission on Digital Development. "Cyber Violence Against Women and Girls: A World-Wide Wake Up Call." September 2015. http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf.

Bureau of Investigative Journalism. "Covert Drone War." Last modified 18 May 2016. https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs.

Butler, Judith. "Violence, Mourning, Politics." *Precarious Life: The Powers of Mourning and Violence*. Verso: 2004, p. 19-49.

Cacho, Lisa Marie. *Social Death: Racialized Rightlessness and the Criminalization of the Unprotected*. NYU Press: 2012.

"catfish." *Urban Dictionary*. Accessed November 2016, https://www.urbandictionary.com/define.php?term=catfish.

Chen, Liyan. "The World's Largest Tech Companies: Apple Beats Samsung, Microsoft, Google." *Forbes*. 11 May 2015. http://www.forbes.com/sites/liyanchen/2015/05/11/the-worlds-largest-tech-companies-apple-beats-samsung-microsoft-google/#18311ac6415a.

Collyer, Megan. "Watch President Barack Obama's 2016 SXSW Interactive Keynote," 12 March 2016. http://www.sxsw.com/interactive/news/2016/president-obama-sxsw-keynote-video.

Cook, Tim. "A Message to Our Customers." *Apple, Inc.* 16 February 2016. http://www.apple.com/customer-letter.

Crash Override Network. "Guide for Employers." 27 Apr 2015. http://www.crashoverridenetwork.com/employers.

----- "Guide For Talking to Family & Police." 15 Mar 2015. http://crashoverridenetwork.tumblr.com/post/113748237272/guide-talking-to-family-police.

----- "So You've Been Doxed: A Guide to Best Practices." 21 March 2015. http://crashoverridenetwork.tumblr.com/post/114270394687/so-youve-been-doxed-a-guide-to-best-practices.

Davies, Rob. "US corporations have 1.4tn hidden in tax havens, claims Oxfam report." *The Guardian.* 14 April 2016. http://www.theguardian.com/world/2016/apr/14/us-corporations-14-trillion-hidden-tax-havens-oxfam.

Electronic Frontier Foundation. "How the NSA Domestic Spying Program Works," *Electronic Frontier Foundation.* Accessed 26 February 2016. https://www.eff.org/nsa-spying/how-it-works.

Eler, Alicia and Brannon Rockwell-Charland. "Naming a Radical Queer Girl Tumblr Aesthetic." *Feminist Journal of Art and Digital Culture*, iss. 32 (2015). https://dpi.studioxx.org/en/no/32-queer-networks/naming-radical-queer-girl-tumblr-aesthetic.

Frank, Allegra. "Pokémon GO heading out to the field in Japanese-only beta test." *Polygon.* 4 March 2016. http://www.polygon.com/2016/3/4/11161010/pokemon-go-field-test-beta-japan.

Fuchs, Christian. "The Political Economy of Privacy on Facebook." *Television & New Media* vol. 13 no. 2, March 2012.

Fussell, Sidney. "How Facebook, Instagram, and Twitter helped police target black activists." *Fusion.* 12 October 2016. http://fusion.net/story/356808/facebook-twitter-instagram-geofeedia-tracking.

Gannes, Liz. "The Short and Illustrious History of Twitter Hashtags." *Gigaom.* 30 April 2010. http://gigaom.com/2010/04/30/the-short-and-illustrious-history-of-twitter-hashtags.

Gellman, Barton and Laura Poitras. "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program." *The Washington Post.* 7 June 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Gellman, Barton, Julie Tate, and Ashkan Soltani. "In NSA-intercepted data, those not targeted far outnumber the foreigners who are." *The Washington Post.* 5 July 2014. https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

Grant, Rebecca. "Google tried to resist FBI requests for data, but the FBI took it anyway." *VentureBeat.* 6 June 2013. http://venturebeat.com/2013/06/06/google-tried-to-resist-fbi-requests-for-data-but-the-fbi-took-it-anyway.

Greenwald, Glen and Ewan MacAskill. "NSA Prism program taps in to user data of Apple, Google and others." *The Guardian.* 7 June 2013. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Hammonds, Evelyn. "Black (W)holes and the Geometry of Black Female Sexuality." *differences* 6: 2+3. Indiana University Press, (1995): p. 126-146.

Harris, Anita, ed. *All About the Girl: Culture, Power, and Identity.* New York: Routledge, 2004.

Hauslohner, Abigail and Ashley Cusick. "Alton Sterling's relatives weather scrutiny, call for justice." *The Washington Post.* 13 July 2016. https://www.washingtonpost.com/national/alton-sterlings-relatives-weather-scrutiny-call-for-justice/2016/07/13/dbf0ba60-490f-11e6-bdb9-701687974517_story.html.

Hernandez, Daniela. "This is How Computers See Porn." *Fusion.* 30 June 2015. http://fusion.net/story/158507/this-is-how-computers-see-porn.

Jeong, Sarah. "'I'm Disappointed': Zoë Quinn Speaks Out on UN Cyberviolence Report." *Vice Motherboard.* 1 Oct 2015. http://motherboard.vice.com/read/im-disappointed-zoe-quinn-speaks-out-on-un-cyberviolence-report.

Johnston, Casey. "Chat logs show how 4chan users created #gamergate controversy." *ArsTechnica.* 9 September 2014. http://arstechnica.com/gaming/2014/09/new-chat-logs-show-how-4chan-users-pushed-gamergate-into-the-national-spotlight.

Joseph, Miranda. "The Performance of Production and Consumption." *Social Text* (1998): 25-61.

Kalra, Aparna. "Making the cookie crumble differently." *Business Standard.* 2 December 2013. http://www.business-standard.com/article/companies/making-the-cookie-crumble-differently-113120200046_1.html.

Kim, Arnold. "Apple's Media Event to be Held the Week of March 21st, not March 15th." *MacRumors.* 27 February 2016. http://www.macrumors.com/2016/02/27/apple-event-march-21-week/.

Lichtblau, Eric. "Judge Tells Apple to Help Unlock San Bernardino Gunman's iPhone." *New York Times.* 16 February 2016. http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html.

Lister, Martin, et al. *New Media: A Critical Introduction.* Routledge, 2008.

Lone Hill, Dana. "Facebook Don't Believe in Indian Names." 2 February 2015. http://lastrealindians.com/facebook-dont-believe-in-indian-names-by-dana-lone-hill.

Lundby, Knut, ed. *Digital Storytelling, Mediatized Stories, and Self-representations in New Media.* New York: Peter Lang, 2008.

Lyonnais, Sheena. "Anita Sarkeesian Responds to Beat Up Game, Online Harassment, and Death Threats on Stephanie Guthrie." *Toronto Standard.* 10 July 2012. http://www.torontostandard.com/industry/exclusive-anita-sarkeesian-responds-to-beat-up-game-online-harassment-and-stephanie-guthries-death-threats.

MacAskill, Ewan. "NSA paid millions to cover Prism compliance costs for tech companies." *The Guardian.* 23 August 2015. http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

Magnet, Shoshana Amielle. *When Biometrics Fail: Gender, Race, and the Technology of Identity.* Duke University Press Books: 2011.

"Market Share of the Most Popular Social Media Websites in the U.S. in October 2016." *Statista.* Accessed October 2016. http://www.statista.com/statistics/265773/market-share-of-the-most-popular-social-media-websites-in-the-us.

Menn, Joseph. "Yahoo secretly scanned customer emails for U.S. intelligence." *Reuters.* 4 October 2016. http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT.

Morrison, Aimee. "Facebook and Coaxed Affordances." *Identity Technologies: Constructing the Self Online.* Madison, Wisconsin: The University of Wisconsin Press, 2013.

Nakamura, Lisa. *Cybertypes: Race, Ethnicity, and Identity on the Internet.* New York: Routledge, 2002.

----- *Digitizing Race: Visual Cultures of the Internet.* University of Minnesota Press, 2008.

National Institute of Justice. "Predictive Policing." 9 June 2014. http://www.nij.gov/topics/law-enforcement/strategies/predictive/policing/Pages/welcome.aspx.

"Nintendo market value doubles on Pokémon GO mania." *The Guardian.* 19 July 2016. https://www.theguardian.com/technology/2016/jul/19/nintendo-market-value-doubles-on-pokemon-go-mania.

Obama, Barack. "President Obama's full Oval Office Address." *CNN.* 7 December 2015. http://edition.cnn.com/videos/us/2015/12/07/president-obama-oval-office-terror-speech-full.cnn.

The Official Pokémon Channel. "Discover Pokémon in the Real World with Pokémon GO!" 9 September 2015. https://www.youtube.com/watch?v=2sj2iQyBTQs.

Peterson, Andrea. "Why the Philando Castile police-shooting video disappeared from Facebook—then came back." *The Washington Post.* 7 July 2016. https://www.washingtonpost.com/news/the-switch/wp/2016/07/07/why-facebook-took-down-the-philando-castile-shooting-video-then-put-it-back-up.

Perez, Sarah. "Pokémon GO becomes the fastest game to ever hit $500 million in revenue." *TechCrunch.* 8 September 2016. https://techcrunch.com/2016/09/08/pokemon-go-becomes-the-fastest-game-to-ever-hit-500-million-in-revenue.

Phillip, Abby. "Online 'Authenticity' and How Facebook's 'Real Name' Policy Hurts Native Americans." *Washington Post – Blogs.* 10 February 2015. https://www.washingtonpost.com/news/morning-mix/wp/2015/02/10/online-authenticity-and-how-facebooks-real-name-policy-hurts-native-americans.

Pokémon GO! Published and developed by Niantic, Inc. 2016.

"Pokémon GO Servers." *Know Your Meme*, submitted by user C_Mill24. Accessed August 2016. http://knowyourmeme.com/photos/1144991-pokemon-go.

Puar, Jasbir K. and Amit Rai. "Monster, Terrorist, Fag: The War on Terrorism and the Production of Docile Patriots." *Social Text* 20.3 (2002): 117-148.

Quinn, Zoë. "August never ends." @TheQuinnspiracy. 11 Jan 2015. https://twitter.com/thequinnspiracy/status/554427624248709120.

----- "August never ends." *Zoë Quinn//Unburnt Witch.* 11 January 2015. http://blog.unburntwitch.com/post/107838639074/august-never-ends.

----- "Once Again, I Will Not Negotiate With Terrorists" *Quinnspiracy.* 19 Aug 2014. http://ohdeargodbees.tumblr.com/post/95188657119/once-again-i-will-not-negotiate-with-terrorists.

----- "Why I Just Dropped The Harassment Charges The Man Who Started GamerGate." *Zoë Quinn//Unburnt Witch.* 10 Feb 2016. http://blog.unburntwitch.com/post/139084743809/why-i-just-dropped-the-harassment-charges-the-man.

Robles, Patricio. "Twitter's latest ad experiment: paid trending topics." *Econsultancy.* 17 June 2010. https://econsultancy.com/blog/6099-twitter-s-latest-ad-experiment-paid-trending-topics.

Sarkeesian, Anita. "Harassment via Wikipedia Vandalism." *Feminist Frequency.* 10 June 2012. https://feministfrequency.com/2012/06/10/harassment-and-misogyny-via-wikipedia.

----- "Tropes vs Women in Video Games." *Kickstarter.* May 2012. https://www.kickstarter.com/projects/566429325/tropes-vs-women-in-video-games.

Savage, Charlie. "Obama Administration Set to Expand Sharing of Data that NSA Intercepts." *New York Times.* 25 February 2016. http://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html.

Scott, Joan W. "The Evidence of Experience." *Critical Inquiry* vol. 17, no. 4. University of Chicago Press (1990): p. 773-797.

Shaw, Adrienne. "Do You Identify as a Gamer? Gender, Race, Sexuality, and Gamer Identity." *New Media & Society* 14, no. 1 (2012): 28-44.

----- "Putting the Gay in Games Cultural Production and GLBT Content in Video Games." *Games and Culture* 4 (3) (2009): 228-253.

Singal, Jesse. "Gaming's summer of rage." *The Boston Globe.* 20 September 2014. https://www.bostonglobe.com/arts/2014/09/20/gaming-summer-rage/VNMeHYTc5ZKoBixYHzi1JL/story.html.

Spurr, Ben. "Eulogy for: Beat Up Anita Sarkeesian." *Newgrounds.* 7 May 2012. http://www.newgrounds.com/portal/view/598591.

Stanglin, Doug and Kevin Johnson, "FBI: No evidence San Bernardino killers were part of a cell." *USA Today.* 5 December 2015. http://www.usatoday.com/story/news/nation/2015/12/04/suspects-family-shocked-killings/76773382.

Stanton, Rich. "GamerGate Members Are Responsible for the Terrorist Photograph of Journalist Veerender Jubbal." *Vice.* 17 November 2015. http://www.vice.com/en_uk/read/gamergate-members-are-responsible-for-the-terrorist-photograph-of-journalist-veerender-jubbal-503.

Steiner, Peter, "On the Internet, nobody knows you're a dog" illustration, *The New Yorker*, 1993.

"The Counted." *The Guardian.* Accessed 1 December 2016. https://www.theguardian.com/us-news/ng-interactive/2015/jun/01/about-the-counted.

"thezoepost." Wordpress. 16 Aug 2014. http://thezoepost.wordpress.com.

Tongson, Karen. *Relocations: Queer Suburban Imaginaries.* New York University Press: 2011.

Tumblr meme (origin: @venusisfortransbians). "tumblr dot hell users to support staff." http://venusisfortransbians.tumblr.com/post/149200577599/tumblr-dot-hell-users-to-support-staff.

Tumblr thread (Origin: @transpolarized).
http://lesbianzoidberg.tumblr.com/post/149198684374/lesbian-death-trope-transpolarized.

Tweet by @_EricHu. 9 July 2016.
https://twitter.com/_EricHu/status/751915801750495232.

Tweet by @Bl4ptrep. 14 November 2016,
https://web.archive.org/web/20151114003205/https:/twitter.com/bl4ptrep/status/665323528279855104.

Tweet by @DallasPD. 7 July 2016.
https://twitter.com/DallasPD/status/751271541459984384.

Tweet by @dallasnewsphoto. 7 July 2016.
https://twitter.com/dallasnewsphoto/status/751235966505881600.

Tweet by @jessysaurusrex. 12 March 2016.
https://twitter.com/jessysaurusrex/status/708787029123792898.

----- 2 October 2016. https://twitter.com/jessysaurusrex/status/782751109064433664.

Tweet by @nhlmurphy. 7 July 2016.
https://twitter.com/nhlmurphy/status/751271612637257729.

Tweet by @robfee. 21 August 2016.
https://twitter.com/robfee/status/767606169430921216.

Tweet by @Sickayduh. 13 August 2016.
https://twitter.com/sickayduh/status/764683140417728512.

Tweet by @veeren_jubbal. "#StopGamerGate2014." 14 October 2014.
https://twitter.com/Veeren_Jubbal/status/522185406263988224.

Tweet by @YahBoyEric. 7 July 2016.
https://twitter.com/YahBoyEric/status/751271645742977024.

Twitter. "Privacy Policy." Last updated 27 January 2016, Accessed 17 April 2016.
https://twitter.com/privacy.

Ward, Jackie. "Hidden Microphones Exposed As Part of Government Surveillance Program in the Bay Area." *CBS SF Bay Area.* 13 May 2016. http://sanfrancisco.cbslocal.com/2016/05/13/hidden-microphones-exposed-as-part-of-government-surveillance-program-in-the-bay-area.

Weinberger, Matt. "'Pokémon Go' international rollout will be 'paused' as players overload the system." *Business Insider.* 8 July 2016. http://www.businessinsider.com/pokemon-go-international-rollout-paused-2016-7.

Wingfield, Nick. "Intel Pulls Ads From Site After 'Gamergate' Boycott." *The New York Times.* 2 Oct 2014. http://bits.blogs.nytimes.com/2014/10/02/intel-pulls-ads-from-site-after-gamergate-boycott.

Wu, Brianna. "No skin thick enough: The daily harassment of women in the game industry." *Polygon.* 22 July 2014. http://www.polygon.com/2014/7/22/5926193/women-gaming-harassment.

Yadron, Danny. "San Bernardino iPhone: US ends Apple case after accessing data without assistance." *The Guardian.* 20 March 2016. https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone.