CREEPING BODIES:

Digital Mediation and Embodied Experience — A Series of Three Case Studies

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION
OF THE UNIVERSITY OF HAWAIʻI AT MĀNOA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTORATE OF PHILOSOPHY

IN

POLITICAL SCIENCE

By

Zoe S. S. Vorsino

Dissertation Committee:

Jairus Victor Grove
Nicole Sunday Grove
Jonathan Goldberg-Hiller
Deborah Halbert
John Rieder

Keywords: Security studies, deepfakes, AI, digital culture,

algorithms, critical theory, media studies

Dedication

I dedicate this dissertation to my family. I will always be more than grateful for the patience, care, and understanding you provided me with during my graduate studies. To my father, Donald; you have always been my most unquestioning fan, and it has not gone unnoticed, nor unappreciated. I would have given up many times if not for your unflinching and enthusiastic support. To my sisters, Marie and Lucia; thank you for being the role models you have always been in my life. You both are entirely too cool and entirely too well-adjusted for me to at least try to be anything else. Finally, Bambino, Scooter, Mocha, and Lucky; thank you for providing the comfort, laughter, and distraction that kept me grounded throughout this process.

Acknowledgments

I am deeply indebted to my advisor, Jairus Victor Grove, for his patience, understanding, and invaluable scholarly input throughout both my Master's and Doctoral degree. His guidance and no-nonsense humor not only kept me buoyed, but improved my research. I also could not have undertaken this journey without the advice and generous support of my defense committee; Nicole Sunday Grove, Jonathan Goldberg-Hiller, Deborah Halbert, and John Rieder, who were the cornerstones of my thinking and writing the entirety of my time as a doctoral student at the University of Hawai'i at Mānoa.

I am grateful to my classmates and cohort members of the University of Hawai'i at Mānoa Political Science department, who provided invaluable feedback and a community of learning held to an incredibly high and often theoretically nuanced standard. I am thankful to the peers from all around the world who I had the chance to meet through conferences, panels, and online discussion during this time. I would also be remiss if I did not give thanks to the many students I taught as a Graduate Assistant and Lecturer, who helped me gain confidence as a researcher, teacher, and scholar, and opened my eyes to the multitude of experiences we all approach the world of academia with.

Lastly but no less importantly, I would like to acknowledge my family, who supported me throughout this process, often with more enthusiasm than myself.

Abstract

The modern digital experience is at once creepy yet mundane; surprising yet boring; quotidian and yet extraordinary. Mathematical equations – algorithms – guide our decisions and yet themselves are mired in obfuscated biases around race, gender, and nationality. Body parts are stitched into and around other body parts using deepfake software and puppeteered as they are disseminated along online informational highways. Biological functions are securitized, captured by machinic eyes and judged as risky if they deviate from a standardized, automated biometric system. In this environment, embodiment itself is turned into a parameter in the program of life, expected to work within the confines of any given software design, or be rewritten until it just works. This project takes the form of three chapters, each a case study through which I aim to answer a series of simple questions that seek to illuminate both the seemingly self-apparent and futuristically creepy aspects of the modern digitally embodied experience: What does it mean to be alive in a world where the boundaries between the digital and the corporeal have, for most intents and purposes, become liminal? And in that context, in this new world of digitized embodiment, how does one become entwined in power structures, both new and old?

After an introduction aimed at offering foundational arguments, Chapter Two uses AVATAR as its point of entry in an attempt to complicate the notion of the "e-border" widely imagined by Western security apparati as a solution to post 9/11 security risks (Amoore 2013). Not merely, I argue, does AVATAR present as an assemblage through which the body is digitally dissected (Wilcox 2015) at the hands of a simulated proxy sovereign, but it is indicative of how digital security technologies facialize the subjectification process. In Chapter Three, I step away from the physical borders of the airport to consider Tay.Ai, a chatbot released by

Microsoft on social media platform Twitter in 2016. Tay.Ai was meant to test Microsoft's newest automated algorithmic language engine by interacting directly with internet users – as such, the chatbot was designed to look and have the linguistic habits of an "average American woman" online (Neff & Nagy 2016). Tay.Ai's eventual non-compliance with its programmatic imperatives lets us consider how normative assumptions about gender and race play into software development and user experience, especially in the context of the digital public square that are web 2.0 social platforms. In Chapter Four, I examine the deepfake as a digital object made up, partly, I argue, of the body. Or, at least, the bodies of those captured, dissected, stitched, and edited together to create new forms of digital embodiment. Using a 2018 Buzzfeed PSA depicting President Barack Obama as voiced by comedian Jordan Peele, I consider how race is used as a technology of othering within spaces of algorithmic mediation.

Finally, in a brief conclusion, I consider a politics of refusal in the face (pun intended) of pervasive embodied capture within the machine, paying special attention to current discourse as it applies to both modern conceptions of privacy and resistance.

Chapter One: Introduction

With no shortage of fanfare, Tay.Ai, a female-gendered chatbot designed to show off flashy advances in AI conversational engagement, starts to interact with users on a popular social media platform. Less than a day after going live, the chatbot's avatar — a young (white) woman with a bubbly personality — goes off the rails, spreading conspiracy theories and espousing anti-Semitic views. The experiment is hastily pulled down, and Tay.Ai is touted as a supposed failure of programming (Alba 2016).

A comedian partners with Buzzfeed, an American online media company, to create a PSA campaign featuring President Barack Obama. Only the president depicted in the video that is eventually published isn't really the President. Or rather, it isn't *just* the President. Instead, it is a digitally stitched representation — a deepfake — of the President's body speaking the words of comedian Jordan Peele as he/they extoll on the dangers of algorithmically aided misinformation campaigns. President Obama's famously even-keeled, halting delivery is usurped by statements calling Donald Trump a dipshit and references to Black-American culture.

Funded with government money and touted as "deception detection" technology, AVATAR — Automated Virtual Agent for Truth Assessments in Real Time — receives funding by the U.S. Department of Homeland Security in a bid to supposedly streamline the border crossing process. Automated algorithmic questioning with sanitized on-screen avatars are imagined as the future of the border — and the e-border — building upon previous devices that used AI and biometrics to digitally represent human interaction. The devices' final design is a white, clean-cut man with a standard North American accent – a symbol of American sovereignty presented in contrast to that of the mobile traveler.

Gendered chatbots; racialized deepfakes; simulated white, male border agents. While these examples of algorithm-driven tech in the modern world are seemingly loosely related at first glance, even perhaps, instances of technological gimmicks, they have something fundamental in common: They all deal with embodiment and the way our conception and *experiences* of said embodiment are affected by digital mediation. Whether that embodiment is a matter of discourse and social norms surrounding gender (as I argue in the chapter focusing on Tay.Ai) or a matter of literal facial capture and simulation (as I consider in the chapter on AVATAR), or even a matter of two bodies being digitally dissected and stitched together to form the punchline to an American-specific joke about race and its place in politics (as is examined in the chapter on deepfakes), the technologies covered in this dissertation have been chosen for study in order to highlight the weird, wonky, often nebulous condition of the body as it relates to, reacts to, and is — terrifyingly — consumed by, the digital.

But what are the stakes on hand with a body increasingly defined by the digital? To put it another way, where does the "creep" come into play here? The terror? The horror? The very real consequences of a body defined, increasingly, by numbers and programs and software and math? While Gilles Deleuze (1995) suggests that control, a la surveillance, grows like creeping weeds, and Zygmunt Bauman and David Lyon (2002) suggest that we "think liquid" when it comes to surveilled digital mediation, perhaps the more appropriate term here, at the crossroads of the body and the digital, the warm flesh of embodied life and the terrestrially-strewn wires of digital mediation, is "ooze." What, then, is so terrifying about creeping? About liquid states of mind? About ooze?

In Irvin Yeaworth's 1958 American independent sci-fi horror film *The Blob*, a carnivorous amoebicidal alien crashes to Earth. It envelops everything it touches — biological and inert —

becoming larger and more aggressive as it does so. The danger of the amoeba blob, as it oozes and slimes and creeps, inch by inch, across a small town of Phoenixville, Pennsylvania, is that it will, eventually, consume everything. That this alien form of intelligence that seemingly only exists to become *more*, will continuously get larger and larger and larger until nothing is not part of one giant, gelatinous, mindless blob. The horror jiggling around inside the rounded folds of the blob's bulbous body is this: if the blob consumes everything, then there is nothing that exists outside of it that supports daily life. There is no escape. There are no other options. There is no refusal. There is only a blob; an oozing, creeping amalgam of flesh and trash and wires and a multitude of experiences condensed into one singular need for more. And while anthromorphized chatbots, algorithmically-edited, stitched video-based bodies, and automated security-contextualized avatars may seem far removed from the blobby horrors of an endlessly ravenous extraterrestrial intelligence, I present here that the sublimated danger of these technologies, apart from their more immediate gendered, racialized, and securitized violence, is the creation of conditions through which there is no opt-out button. Through which, as I discuss in the following dissertation, a digitally mediated definition of the body redefines and reconfigures violence, and therefore freedom, control, and power, into a phenomenon from which there is no recourse. Consider, for instance, the Leviathan.

Since Hobbes, freedom itself has been understood in terms of embodiment; it is both unimpeded and removed from the sovereign's gaze. In his words, "in secret free" (qtd. in Epstein 2016, 37). That is, even against the all-encompassing sovereignty of the Leviathan, the non-visible body is the linchpin of the political subject's freedom *and* the basis for their freedom (Epstein 2016, 37). When Hobbes constructed his Leviathan, he was imagining a system of governance — a method of control punctuated by absolute sovereignty, the superiority of

civilization over nature, and an embodied notion of the political (Hobbes & MacPherson 1982). He was also setting the stage, at least in the corpus of Western political theory, for a definition of intelligence (and of utopia) that saw computational and mechanic logic as something that could intervene in the relationship between civilization and nature, human and God, and the body politic and sovereign. The diffuse intelligence of the artificial man described in Hobbes' commonwealth is a kind of self-regulating system, in which human society constitutes a new form of life; an over-arching intelligence made up of its subjects. Hobbes established that logic and digital computation share common foundations, sparking a conversation on the validity of whether reasoning can be reduced to arithmetic—that is, can machines think (Dyson 2012)?

Hobbes' utopia, then, is less concerned with the homeostasis of an embodied subject then with the homeostasis of the body politic as controlled by its own machinations opposed to some transcendent sovereign. Thus, the Leviathan is a self-sustaining system that has more in common with the distributed, mobile networks of the 21st century than it did with even the mechanical automaton intelligences conceived during the 19th and 20th centuries (Dyson 2012). I begin with Hobbes, and the Leviathan, because modern connectivity — or the embodied logics on which modern connectivity is founded — traces its beginnings back to Hobbes' creation. I also find Hobbes useful in elucidating the risk of embodiment defined via a number of technologies, both social and material. If the Leviathan was an early version of theorized artificial intelligence – AI – affecting but not consuming subjects under its vice-like grip of sovereignty, then the blob — a creeping ooze made up of flesh, metal, biohazardous chemicals, and trash, all but suspending its prey in a viscous environment of constant mediation — is its far-future evolution.

This project takes the form of three chapters, each a case study through which I aim to answer a series of simple questions that seek to illuminate both the seemingly self-apparent and

futuristically creepy (and oozy) aspects of the modern digital experience: What does it mean to be alive in a world where the boundaries between the digital and the corporeal have, for most intents and purposes, become liminal? And in that context, in this new world of digitized embodiment, how does one become entwined in power structures, both new and old?

I begin, below, briefly, with the general methodological framing of this project. Next, I foray into the literature, logics, and ideas that scaffold my research. Paralleling the complicated, interconnected, and intersectional nature of the modern digital experience, the literature review that follows covers an array of topics, ranging from surveillance studies to queer theory (e.g. Butler, 2011), to cybernetics (e.g. Wiener, 2013), to Western philosophy (*a la Hobbes* as explicated by Epstein 2008), to critical theory (e.g. Massumi, 2005). This review is not meant to be an exhaustive introduction to my own theoretical approach, but rather a preview, to be later built on in each subsequent case study. That is, I am more interested in *framing* my research in this chapter, both theoretically and methodologically, than reviewing literature. That said, generally, the topics covered in this literature review fall into one of three parts: a discussion of cybernetic theory as a foundational logic for modern computational systems and networks; an examination of surveillance as it is made an intrinsic part of everyday life; and finally, a look at how the body exists in these systems of control and resource extraction.

Chapter Two uses AVATAR as its point of entry in an attempt to complicate the notion of the "e-border" widely imagined by Western security apparati as a solution to post 9/11 security risks (Amoore 2013). Not merely, I argue, does AVATAR present as an assemblage through which the body is digitally dissected (Wilcox 2015) at the hands of a simulated proxy sovereign, but it is indicative of how digital security technologies facialize the subjectification process.

In Chapter Three, I step away from the physical borders of the airport to consider Tay.Ai, a chatbot released by Microsoft on social media platform Twitter in 2016. Tay.Ai was meant to test Microsoft's newest automated algorithmic language engine by interacting directly with internet users – as such, the chatbot was designed to look and have the linguistic habits of an "average American woman" online (Neff & Nagy 2016). Tay.Ai's eventual non-compliance with its programmatic imperatives lets us consider how normative assumptions about gender and race play into software development and user experience, especially in the context of the digital public square that are web 2.0 social platforms.

For my final case study in Chapter Four, I examine the deepfake as a digital object made up, partly, I argue, of the body. Or, at least, the bodies of those captured, dissected, stitched, and edited together to create new forms of digital embodiment. Using a 2018 Buzzfeed PSA depicting President Barack Obama as voiced by comedian Jordan Peele, I consider how race is used as a technology of othering within spaces of algorithmic mediation. Following that, I look at a deepfake meme of Russian President Vladimir Putin to examine digital homononationalism.

Finally, in a brief conclusion, I consider a politics of refusal in the face (pun intended) of pervasive embodied capture within the machine, paying special attention to current discourse as it applies to both modern conceptions of privacy and resistance.

A Word on Methodology

Allow me a brief detour. In 2016, Apple released the first iPhone with a built-in facial identification security system. At the time, Apple was releasing the new model of their flagship device — the iPhone X — with what they hoped would be the first Face ID system that could discern between an actual face, and, say, a picture of a face or even a mask of a face. The goal,

according to chief Apple executive officer Phill Shiller, shared during his Hollywood-esque keynote presentation, was to make personal device security "simple, natural, and effortless" (Bollen 2017). A subsumed part of everyday life, connecting the body — via the face — to identity, and identity to a series of dot-driven data points. In its first few months post-release, Face ID became a trending part of the Western American zeitgeist, with social media users creating a variety of memes using the facial capture system and Apple's Animoji feature, and a few things became apparent (Baig 2017). First, that Face ID did indeed present as part of a larger trend towards biometric-based authentication across a spectrum of consumer "friendly" technologies, and not just a brief novelty in an over-saturated market of technological gimmicks. And second, that the adaptation of technologies like Face ID (and, for that matter, Apple's other body-centric security program, Touch ID), is part of a larger logic espoused by Western technological producers that creates the conditions through which specific methods of subjectification and identification contingent on algorithmic and data-centric infrastructures — namely, those that are based on embodiment — are subsumed into the quotidian.

Face ID is, like many camera-based biometric systems — AVATAR is included in this classification, as are the programs used to capture face and body movement of individuals involved in deepfake videos — focused on, somehow, scanning, capturing, authenticating, and then storing dot-based interpretations of individual facial and body characteristics. Thus, today, you sign into your iPhone by looking at it — since your face is — while captured, graphed, and depth-analyzed via a standardized algorithm — "unique" enough to act as a password. Via Apple's website: "Once it knows you, it knows you. Face ID uses advanced machine learning to recognize changes in your appearance. Wear a hat. Grow a beard. Put on glasses… so even if

your friends don't recognize you, Face ID will." It also makes sure you're paying attention, hiding notifications or lowering volume when your eyes are open and looking at the screen.

All this spec regurgitation is to say that Face ID is Apple paying attention to your face, to, in turn, collect data on when and how you pay attention to Apple. This isn't necessarily a novel, innovative idea, nor does Apple's Face ID tout itself, yet (even eight years after its debut) as technology meant to record unique facial expressions, like the software Affectiva markets to capture consumer reactions to advertisements, or, as mentioned, AVATAR. It does, however, show that increasingly, methods of authentication based on software-based conceptions of facial characteristics are salient identifying technologies. It shows that technological life leaves little room for subjective distance from our machines, from the habits we form to the way we see ourselves to the way we interact with our screen-based interfaces. Face ID's success – its frictionless subsumption into the everyday; a story repeated tri-fold in this research project, with various technologies, to various degrees of success — requires that we not only attempt to understand the technics of these increasingly automated programs and how they affect us, but how such programs are designed, produced, marketed, justified, and maintained. The routinization of technologies that rely, somehow, on some sort of biometric identification, whether in a consumer-centric or security-centric sector, underscores the liquidity of state control and surveillance, alluding to the ease with which data extracted for one purpose can be more easily deployed in another. As David Lyon suggests in *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, surveillance within modern networks grows less like a tree — rigid, with a predictive verticality; panoptic — and more like creeping weeds (2002). And, of course, when considered in the context of digital mediated embodiment, it gets a bit more oozy.

Furthermore, algorithms — those that exist within biometric systems, as well as those we experience merely by going on any given social media website — don't appear independent of human intervention. Instead, they often incorporate the prejudices of industry-level expertise, historical trends in data collection, creating the conditions of possibility through which new forms of discrimination automate, rather than do away with, institutional biases (Lyon 2002). Software developers are not entities independent of the sociopolitical zeitgeist — the gendered and racialized quotidian insinuates itself into the job of programming in both technics and corporate structure. Think of, perhaps, Google's move to teach its artificial intelligence engines to be "more conversational" by feeding them romance novels, a move that puts heteronormative ideals and narratives at the forefront of the neural network's role as a good communicator (Hay 2019). Or, as Shoshana Amielle Magnet shows, the prevalence of debunked conceptions of race as incorporated into facial recognition technology: "[Images are labelled] according to [the programmers] own biological race and gender identities (2011);" preconceptions about gender and race are codified into biometric scanners from the very beginning. These are inputs with effects contingent on their specific political modality, and, especially in an age when programming, software, algorithms, and, more generally, automation, are seen as the objective du rigor, it is imperative that the work put into them be cognizant of that. This requirement is made more necessary when the technologies in question amplify and intensify the visibility of their subject.

This dissertation works through the relationship between body, machine, and state, and as such my work sits at the juncture of thought focused on embodiment, affect theory and surveillance, all approached via a feminist methodology that focuses on intersectional experience. A feminist approach, especially, critiques surveillance in order to find out how ruling

relations are enabled by texts and classifications, and how, similar to David Lyon's conception of liquid modernity, techniques conventionally considered to be in the realm of monitoring and documentation reinforce gendered, sexed, raced, and classed exercises of power (2002). As I've just suggested, there is no way to neutrally keep records; to create objective archives independent of computation's militarized and gendered origins. Data collection is not free of functional imperative, and, echoing Mark Andrejevic's thoughts in the *Feminist Surveillance Studies* reader, it becomes necessary for surveillance studies to analyze and explode the interests, pressures, prejudices, and agendas "obscured by the technocratic alibi of the algorithm and its analogs" — control in the name of security, efficiency, and the simultaneous obscuring of discrimination these techniques advance (2015).

Additionally, throughout this dissertation, I use cultural artifacts to make sense of the relationship between us and our machines. In everyday discussions of technology, fiction — and especially science fiction — is used as a method through which to conceptualize and make sense of the rapid shifts of cultural mimesis. I echo this trend to consider how science fiction (or SF) is often used as a conceptual linchpin through which to think through digital life. SF can either invoke paranoia or technophilia in the face of ubiquitous data-centric technology, and thus, ubiquitous surveillance, which makes it a particularly useful lens to think through not just surveillance, but through our reactions to it as well. Steven Shaviro suggests that SF's usefulness arises from its "futuring" of the mundane (2016). Gilles Deleuze suggests that like philosophy, science fiction deals with concepts yet to have been worked out (1995); echoing Darko Suvin's conceptualization of the genre of science fiction, Carl Freedman argues that SF works as a theoretical tool by enacting a kind of 'cognitive estrangement' that works to make visible the contingencies of the modern system; and, he continues, SF attempts to help individual subjects

gain a sense of place in that same system (2000). The speculative nature of SF presents, that is, an easy inroads into extrapolating into the future in a sort of non-temporal way; the future, here, isn't necessarily about time but distance. The type of distance that allows for theory and speculation to be unhindered by the minutiae, and for problematics to be exploded into bombastic, spectacular, view. While SF can be remarkably useful as a critique of modern problems, especially as to their extrapolatory futures, in popular culture it can also inure us to infractions on our experiences even as they exist as hypotheticals.

Here, we return to the banality of the iPhone X and its face tracking technologies. There is a startling continuity across algorithm-centric technologies rationalized via the efficient collection of information, and, as argued by Shosana Magnet's analysis of biometric systems, there is also more to be said about the "normal" functioning of data collection as failure (2011). Irrespective of system "abuses" and/or whether or not hackers, eventually, figure out how to use Face ID to access personalized data (nor the ways in which official security forces in the West are able to circumvent privacy laws using Face ID) the more interesting questions are: What does the everyday-ness of this technology *do*? In terms of subjectification? Control? Surveillance? Privacy? How are those affects intensified, or compounded by, their design? And, indeed, how does *how we conceptualize* these technologies as they are released for consumer purchase, change our experience of them? In that vein, with this dissertation, I consider the relationship between body and technology by paying special attention to materiality, relationality, and process, in turn showing how certain algorithmically inspired sensibilities enact particular forms of knowledge and thus, act as a performance of their own political effects (Aradau and Huysmans 2014).

The Security Question: Science Fiction and Cybernetics

Recently, in a conversation with students in an undergraduate political science course, I brought up the topic of securitized pre-emption, affect, and machine vision. They were nonplussed at my descriptions of FAST, the DHS airport assemblage designed to ascribe intent in a bid to separate dangerous travelers from safe ones, and more so when I showed a video of AVATAR, the biometric interrogation bot tested on the Arizona-Sonoran border. While these examples are factual and from everyday life, many used science fiction — as I did at the beginning of this introduction — to conceptualize and understand the theories and policies I was describing. Among the comments: "Isn't that the plot to Minority Report?"; "I read a dystopian novel like this once;" "So, [Orwell's] *1984* is actually a thing?"). They also, in the same discussion, brought up the ubiquity of biometric scanning in their day to day lives, the social imperatives of online visibility, and the catch-22 of data collection.

To be sure, as Donna Haraway (2006) eloquently concludes, in a world of ubiquitous connectivity, the "boundary between science fiction and social reality is an optical illusion." After all, our lives and bodies are being transformed in ways — and by… oozing… technologies — that seem to invoke the necessity of science fiction as a conceptualizing tool. That is, to list a few heavy questions that preceded the research in this dissertation: What does modern surveillance look like? In what ways does modern surveillance define and benefit from the discourse of privacy? And what does a more critical look at privacy do to a politics of resistance?

To be sure, any conversation about surveillance, pre- or post-Snowden, seemingly always revolves around the violation or protection of privacy. Overwhelmingly, surveillance studies texts set the stage for an Orwellian conflict over increasingly intimate forms of state control and visibility in the form of biometrics and data collection. My own research, especially Chapter

One, an analysis of biometrics in economies of affect and control, is included in this epistemological binary. And, as I mentioned, since Hobbes' explication of the all-seeing, all-knowing Leviathan as state, there has been an intimate understanding and discursive alignment between invisibility and freedom — autonomy and opacity.

What Hobbes does for a conversation about control, intelligence, and machinic thinking works as a precursor to the modern formalization of logic as computative. The axioms of logical programming, of a contingent kind of intelligence, are embedded in the devices and technologies that, increasingly, work to construct worlds and steer populations (either at the behest of hegemonic entities or via their own internal dispositifs). Looking at Hobbes not as the theorist behind the concept of the commonwealth or as the oft-touted founder of modern political science, but as a cyberneticist before cybernetics existed suggests a different picture about the chronology of Western political history. That history — one of cybernetic entreaties against assumed entropy, is also one of utopian promises, and that any discussion of digital embodiment within the context of Web 2.0 spaces as new, or innocuous, or empowering, is built upon this same idea.

The term cybernetics, coined (independent of each other) by both French electrodynamicist Andre-Marie Ampere in the 18th century and Norbert Wiener in 1947, refers in this context to the steering of populations, and, more specifically, to the steering of populations via their relationship to information, communication, and control (Wiener 2013, 11). As Hobbes posits, the various mechanisms by which this control occurs relies on some sort of system or intelligence that steers via machinized logics of communication. Some examples: In *New Atlantis*, Francis Bacon imagines an "ideal space governed by education, inductive reasoning, and empirical experimentation" (Halpern 2014, 9). Similarly, Jeremy Bentham

considered the panopticon an ideal link between visuality, the calculated management of space, and a democratic, lawful government (Halpern 2014, 9). It would provide, he argued, a space in which power could be wielded without force as part of a "utopian reconceptualization of politics. Even Delgado's work with stimocievers was done so in the name of a "psycho-civilized" society" (Delgado 1970).

Indeed, Norbert Wiener (also; cybernetics in general) imagines worlds where there is nothing left unknown — just the constant archival process of recombining, analyzing, and processing. And, to an extent, these dreams have been realized via the ubiquity of personal computation and the pervasiveness of data networks. Technologies such as these create, or at least aim to create, a kind of world — and lived experience — where there is no unknown left to discover. Where everything can be codified, informatized, and archived, and our relationship to time, documentation, and information has been reconfigured via the concepts of communication and control (Halpern 2014).

Cyberneticians concern themselves with process, not essence. Thus, for instance, in rethinking defense while working at MIT's RAD lab, Wiener and his colleagues argued that human behavior could be modeled and predicted — particularly when the subject is under stress. Both machines and humans, he argued, share mathematics as a common language and thus their behavior can be altered using the same principles (Halpern 2014). From this, early efforts to rethink defense and security in the context of communication and behaviorism sought to treat wartime pilots as machines, enemies as "cold-blooded, machine-like opponents," and brought forth a new mode of technical thought where emphasis was placed on *process*, not essence *(ibid).* With this notion came the black box, in which tools of war (think guns, planes, soldiers) were

viewed in terms of their behavior, while their international organization was left unseen and considered unimportant.

The onus on result, rather than function, is also taken up by Wendy Chun in her work on programming and computation, where she argues that the usurpation of the graphic user interface over computer hardware and source code belies a militaristic history through which command must always equal control—the process, again, remains unimportant and for that matter, inaccessible (Chun 2011, 49).

Indeed, the concept of the black box describes a world in which processes are exportable, mobile, and removed from their "initial sites of inception" (Halpern 2014, 42). Chun argues this opacity, or lack of inaccessibility, is intensified in an era in which artificial intelligence, programming languages, and algorithmic processes constitute daily life and governance. Thus, programmers, computer scientists, and theorists have reduced software not to an ontology in and of itself but to a recipe, a set of instructions to make real a targeted outcome, to substitute space and text for time and process. (Chun 2011, 21).

The algorithm – the scaffolding that undergirds the modern digital experience -- perhaps is the black box *par excellence*. In the context in which algorithms (via apps, services, etc.) are now employed, our relationship with computational systems is more than *trust*. Rather, the memetics of these technologies and services work to entrench the idea that big data, ubiquitous sensors, and other types of machine learning can "beneficially regulate" a variety of complex, mobile systems; that user-matching algorithms on dating apps, for example, can find us true love (or a satisfying hook-up), that Spotify can curate the music we listen to according to our tastes; and that Amazon knows what we should buy before we buy it.

Put another way, algorithms require *faith*. The theological connotations here are not by accident. There is, indeed, a kind of theology in the abstraction of source code. Chun uses the image of the *fetish,* originally an object of worship, to consider the false causality of programming and algorithmic logics and explore how it can work to substitute "images for causes (Chun 2011, 50)." In the same vein, Benjamin Bratton warns against the dangers of algorithmic (and, more generally, programmatic) abstraction by considering the speculative implications of *theointerfaciality,* a kind of mobilized opinionlessness, in which no real interpretation is required of the apps and newsfeeds that steer our lives (Bratton 2011, 241). In this environment, chatbots like Tay.Ai, the central figure of Chapter 2, are assumed to be innocuous except for when they do not perform within programmed perimeters.

Theointerfacial technologies augment the world and therefore our understanding and treatment of that world more than they augment vision, or shopping habits, or social interaction. These technologies become a medium, a platform where cognitive processes and the politics within them are increasingly led through and by software-contingent logics, thus creating the conditions of possibility through which it becomes increasingly difficult – not to mention undesirable – to access, understand, and question the system we live in. This has consequences in terms of general ideology and epistemology as well as governance.

Not understanding the algorithms Spotify uses to compile personalized music playlists or Google uses to deliver your search results may not necessarily be dangerous, but it is indicative of a wider acceptance of function without a focus on process. The inability to access algorithms, or at least to have more control over algorithms, becomes inherently problematic in the context of wide-scale biometric databases. Magnet Shosana, in *When Biometrics Fail,* works through the failures of biometrics as inherent to the technology itself — programmers encode images based

on independent understandings of race and gender identities, thus making the inscrutability of the algorithm a mechanism through which identity is standardized, and alterity is ignored (Magnet 2011). The algorithm, as encoded black box, precipitates a subject unaware of the ways they are being categorized, archived, sorted, and treated as a form of embodied human capital. As a blob within a blob wrapped up in wires and tattooed with math.

Feedback: The Body As Information

My conception of embodiment in relation to body-capturing technologies follows from N. Katherine Hayle's experience of the posthuman, wherein no essential differences between bodily existence and computer simulation, or cybernetic mechanism and biological organism, exists. The posthuman embodied subject is an amalgamation of heterogeneous components, where ebbs and flows contend for somatic hegemony and identity is a matter of relational feedback between body and machine (Hayles 1999). Any kind of embodiment-defining computer system has just as much of a chance at validating a kind of performative response as it does in authenticating them. Judith Butler argues that the performative produces what it names, working to create a reality through ontological effect (2011). Discourses and the materialities of the body are both, to an extent, imposed upon, and both possess generative capacities. As a model of embodiment, this helps in thinking through the body as both material and cultural; as both produced by and productive. The technologies of expression tracking, both institutional and material, constitute an entangled process by which definitions of, and reactions to, affect are reified through a recursive, interdependent relationship between machine, institution, and body.

The body in cybernetics is a medium through which data, as information, is read. This instantiates a kind of mechanical patterning, a relationship between machine and body that is

based on control via empirical notions of homeostatic functioning. As Wiener explains, cybernetic control and communication — via the kind of black box algorithms, programs, and software discussed in this research project; social media based chatbots (Chapter Three); automated e-border agent avatars (Chapter Two); widely disseminated deepfakes (Chapter Four) — are all based off feedback (Wiener 2013). The bodies in them are a post-human conflagration of information and flesh, wires and organs, pixels and skin; discursive ideas and ontological realities.

In a particularly technical section in *Cybernetics*, Wiener outlines the mechanical and homeostatic advantages of systems based on feedback and oscillation. His case studies range from mechanical observations of feline quadriceps extensor femoris muscles (or hind thighs) to descriptions of signal towers to the steering of a ship (2013, 19). What remains consistent throughout his analysis is a (normative) conflation between the human body and the mechanical along with an attempt to use the term as a way through which communication and control can be standardized across systems.

Thus, as Hayles suggests, cybernetics has contributed to information losing its body, and, vice versa, to bodies losing their embodiment. The cybernetics push of the mid-20th century also coincided with an emerging realization of the "quantifiable and commodifiable" nature of information that saw it being used in communication theory as a concept cut loose from lived experience (1999, 12). Hayles, in *How We Became Posthuman*, argues that the Macy conferences, where Wiener and his peers worked through their cybernetic vision, have also proven to be a concerted effort to "erase the embodied nature of information through abstraction" (1999). Put another way, bodies are now treated as mediums of information that can be read (across systems).

The datafication of the body is obvious when considering the widescale acceptance of the Quantified Self, for instance. Fitness trackers, mail-in DNA tests, heart rate monitors, and technologies like them aim work to create a kind of self-disciplined subject that oscillates and maintains their own ideal form via feedback from devices that, in themselves, are the result of a notion of computation that derives its meaning from Cartesian conceptualizations of logic and order (Munster 2006). This back-and-forth subjectification — power and control oscillating around feedback — is, as well, a main component of not just quotidian technologies that aim to better know, for instance, what bacteria your gut is composed of, but is also a foundational imaginary behind the design of AVATAR (Chapter Two), the automated e-border agent that projects a particular image of sovereignty to mobile travelers. The quantifiable individual is always already subjected to systems of control; securitized and scrutinized according to the logics of a black-boxed program.

Bratton, in *The Stack: On Software and Sovereignty,* questions what effects the quantifiable nature of subjectivity has on the individual: "[This movement] seeks to use data capture technology to track an individual User's 'inputs' (i.e. food and air), 'states' (mood, energy level,' and 'performance' (mental and physical metrics) … For the User, [it provides recognition and misrecognition, not so unlike Jacque Lacan's mirror stage parable" (2016, 263). Bratton further asks whether—as result of this extreme form of individuation — we will "become even further atomized, grotesquely over-individuated as we stare dumbly into our own templated reflections of profiles, feeds, and complimentary feedback, or will we become even more hive like (ibid.)."

Communication and Control: Engineering Subjects

In a short, bombastic, and oft-cited postscript published in *October*, Giles Deleuze recognized a conflict of sorts between societal institutions and social technologies, prescribing a historical usurpation of societies of discipline by societies of control. Discipline societies, he puts forth, are based on the static isolation and demarcation of different infrastructures (the school, the prison, the factory), while control societies are defined by the mobility afforded systems of control via networked technologies (Deleuze 1992, 3). The corporation replaces the factory; perpetual training replaces the school; the individual becomes the dividual. Indicative to the type of control society that Deleuze talks about are mechanisms through which this control becomes a matter of habit. How control becomes self-actuating.

In order for control societies to work, then, a certain relationship between subject and state needs to be realized — one in which control itself becomes a self-perpetuating system. Karl Deutsch, writing before Deleuze, explains "cybernetics … represents a shift in the center of interest from driving to steering, and from instincts to systems of decisions, regulation, and control (1963)."

Put another way, the mobility of modern computation—whether in the literal sense of mobile devices or in the multi-use functions made possible via algorithmic and programmatic specialization — creates conditions under which these technologies become a kind of infrastructure of control, steering the everyday experience via a relationship based on feedback between the individual and the graphical user interface. The curation of *everything* — from casual hook-ups and music preferences to participation in governance and how we walk through airports and borders — is done via algorithmic systems of individuation.

In his examination of the control society, Deleuze presents an interesting question about the context of control itself, especially the kind of control instantiated by a network of data and data-driven programming. As Roman satirist Juvenal asked: *Quis custodet ipsos custodes*? Who watches the watchmen? And in the context of this study: Who or what controls control? What processes supersede those of the algorithm? Mathew Fuller and Andrew Goffey argue that the recursiveness of control mechanisms in new media makes it so no upper layer is necessitated (2012). Recursive programming controls control via stacked levels of control — "when control controls controlling, control is formally dexterous enough to conjugate itself, endlessly (Fuller & Goffey 2012, 76)." In other words, it becomes automatic, solidly entrenched in the perceptual, affective, and epistemological experience. That is, it acquires a kind of agency all its own.

Thus, technologies as ubiquitous as the face ID on your smartphone or as flashy as the dual face-scanning/virtual aquarium tunnel installed at Dubai International Airport (Craggs 2017) perpetuate themselves, in some sense independent of any political or technological labor that goes into them. Control in this milieu has no identifiable center — it exists in the affective and subjective experiences instantiated by interacting with these technologies. In examining this control we might consider Louis Althusser, in "Ideology and Ideological State Apparatuses," who proposes the concept of interpellation (2014). He describes a scene in which a police officer hails an individual by yelling, "Hey, you there!" The individual turns around and *in that moment* becomes a subject. The gesture of turning shows that they have recognized themselves as someone to be hailed, regardless if they are guilty of a crime. Althusser argues this acts as a kind of allegorical model of ideology, which consists in forcing populations to freely recognize the authority of the law, and thus become subjects (2014).

Similarly, Didier Fassin helps us understand how interpellation can coincide with Foucauldian interpretations of power (2013). In one sense, the process is one of subjection — wherein the individual submits to domination by some kind of sovereign — and in another, it is one of subjectification, wherein the individual then constructs himself through this identification. But there is also a different kind of interpellation made possible through algorithmic technologies which treat the body as data. In this framework, it is not necessarily a matter of individual acts or incidents that perpetuate the power of the state over the subject, but rather the pervasiveness of these technologies, which in many instances become part of the security state assemblage and make us aware of ourselves as embodied within systems of capture.

Thus, Edward L. Bernays, in *The Engineering of Consent* (1947) and *The Manipulation of Public Opinion* (1928), considers the loci of manipulation in the *treatment* of the subject, concluding technologies that individuate do more in engineering the subject to accept this authority as legitimate. After all, when a traveling body is scanned at an airport while walking through that novel aquarium tunnel, or when race is used as a technology of othering in a widely disseminated deepfake PSA, there is no officer yelling, “Hey, you,” Rather, the system of networked technologies seeking to discern the dangerous from the innocuous, the us and the them, are disparate and, for the most part, unseen. Put another way, the kind of hailing made possible now is an uncomfortable measure of visibility — it exists in the creepy moments of what Benjamin Bratton calls the reverse uncanny valley, where we are momentarily made aware of what we look like through a machine’s eyes (Bratton 2015). A machine that is, intrinsically, linked to hegemonic systems of resource extraction and social organization.

Surveillance Culture: Embodied Monetization

Building off the idea of Deleuze's control society, the surveillance society, as a concept, helps us consider the consumerized instrumentalization of affect into dispositifs of surveillance. Specifically, the focus here is on the commodification and "user-friendly" aspect of data collection as indicative of a larger move towards function creep, emphasizing the danger in the assumed distance between soft and hard surveillance. These studies undergird my larger intellectual aim, which is to point to the way that the body, and the affective responses that body creates, are treated as data through which to control populations and engineer subjects. The three case studies I present in this project all deal with embodiment, surveillance, control, and the dissemination of information within different contexts — the liminal and highly securitized space of the airport; the seemingly "innocuous" public square that is social media; the posthuman stitching of body parts and algorithmic equations in deepfake videos — however they all exist within a highly networked environment through which everything is always already surveilled, securitized, monetized, and archived.

The kind of surveillance in which technologies like expression tracking, chatbots, and deepfakes are deployed are more than an aspect of modern culture; they are an architecture. Jonathan Crary, in *Suspensions of Perception,* argues that mobile computers work as antinomadic procedures; methods for the management of attention (2001). He continues: "[They] use partitioning and sedentarization, rendering bodies controllable and useful simultaneously, even as they simulate the illusion of choice and interactivity" (2001, 75). The ubiquity and striating tendencies of interfacial life (via computation) necessitates that surveillance is not only an over-extension of state power. Surveillance is not just practiced *on* us; we participate *in* it. And, this participation, this so-called surveillance society, rose simultaneously with the post 9/11

intensification of security surveillance — ironically, its main carriers, social media and mobile devices were (and still are) promoted as technologies of "freedom and fun" (Lyon 2015).

Pre-Snowden, few connections were made between, for instance, the NSA and Facebook, or prominent Telecom companies and the mass collection of data of their customers. And yet, as shown by the Snowden leak, government security apparatuses depend heavily on data gleaned social media and cloud services. The architecture of surveillance society is that we, through the daily interfacial and commodity needs of the modern experience, willingly share information in the online public domain (Lyon 2015). To be sure, the participatory aspect of the modern interface raises another question this dissertation aims to grapple with: How do we live in this technological contradiction, in which we both use these technologies for enjoyment while remaining cognizant of the ways they make something like mass surveillance and mass embodied instrumentalization possible? By extension, how is something like an attention economy salient to a discussion of surveillance biometric facial tracking?

One key point: Casual digital labor is profitable. Facebook's value, at its peak, was $560 billion. Yes, this value was linked to financial speculation, but it's also due to the company's collection of user data (Collis, et al 2021) — human sociability rendered into capital and then sold (for the most part) to third-party advertisers. These advertisements are then targeted to users based off their news feeds, Google search history, and visited websites. It's a kind of data doppelgänger (Watson 2014). Crary (2001) argues that considering you-as-data is an identification of a purely commodified (perhaps objectified) subject, defined through interactions with the mobile technologies that both control and prove useful.

Certainly, digital labor (as an extension of commodification and exploitation) isn't new theory. Marx distinguished between necessary labor time and surplus labor time in 1867. Richard

Ohman, in *Selling Culture: Magazines, Markets and Class at the Turn of the Century*, identifies magazine advertisements as imperative to American culture beginning in the early 20th century (1998). And, in 1981, Dallas Smythe suggested the "pre-digital" ad-subject — as audiences commit unpaid time and in return watch TV with ads. What's different about digital labor is not the mode of advertisement (Instagram and Facebook ads are not *novel* as much as they are *adapted)* but the intensification of state control (or, *possibility* of control), a redefinition of work versus leisure time, and the wonky embodied politics of the social-digital technologies that actualize this current epoch of embodied monetization.

The constant access to information afforded by the internet creates an economy that produces capital 24/7, and in Crary's conceptualization (2014), makes sleep — not to mention normal daily functioning — a mere roadblock to higher returns and the continuation of a state-subject relationship formed through identity standardizing software. Does this mean, necessarily, that the internet as it stands (the access to networks and connected life) is inherently an architecture of state control? Do the big data tendencies of Google, Facebook, Apple, and Microsoft in the West go as far as to create a kind of platform capitalism/security state? While the connection between data collection and securitized surveillance started off as serendipitous (convenience afforded by a strand of code that allowed websites to remember previous visitors), monitoring is now part of the system and not the exception (Crary 2014).

Here again, I turn to fiction for a way to understand the individual's place in all this. In *Discognition*, Steven Shaviro (2016) suggests, during a discussion of Ted Chiang's *Software Objects,* that the protagonists of the story – digients that live in an online virtual world – are characterized above all by their playfulness and curiosity. Their sentience is more about feeling than cognition and, he continues, their actions are gratuitous rather than functional. They can't be

monetized — a foil, perhaps, to the modern condition of digital labor resides in finding spaces of un-monetized play. He continues that modern accounts of the mind are functionalist and cognitivist — i.e., that cognition is necessary for affective arousal. Against this, Shaviro suggests that *Software Objects* presents a situation in which the cognitive skills of the digients are secondary to their emotions and that it is through adventures of affect in which cognition is learned.

Shaviro's claim here certainly proves a useful tactic in the privileging of cognition over affect, one that requires accepting that commodification on the part of a network of technologies requires cognition on the part of the subject. That conclusion is rife with disagreement, however, as embodied datafication reduces individuals to flows of averages and statistics, and not necessarily, cognition. Giorgio Agamben, in *Homo Sacer* (1998), explicates the biopolitical notion of *zoe* as bare life — life reduced to a biological function. And in the context of networks of commodification and surveillance, the subject (as individual) is approached as such. Indeed, the biometric assemblages of the airport target the biological functions of the human body – heart rate, gaze, temperature, facial tics and movements of muscle. Chatbots distill human speech to logic equations. Deepfakes dismember bodies made of flesh to create digital amalgamate bodies made up of a multitude. The problem is, exactly, that cognition is *not* required. That cognition is not inherent to any kind of monetization process – that indeed, the only thing required for the monetization of the modern digital body is an *idea* of a body itself. And, at that, not necessarily one that is currently alive.

The Politics and Cinematics of the Face

As further studied in Chapter One, even the face does not, necessarily, require a cognizant subject to be mired in programmed systems of control. The face is frozen, captured, predicted and archived. Deleuze and Guattari's concept of faciality imagines faces as frozen aspects of Western culture — separated from the minds behind them (1987). In that way, the usage of "the face," as it refers to how our faces are perceived and conceptualized reveals the inescapable embodiment of a kind of visibility — giving materiality, and physicality, to the political. The face is, in a way, cinematic. A spectacle through which the curtains of a Foucauldian security *dispositif* slowly open.

To Foucault (1995), security is an apparatus — a *dispositif* — and the kind of governance that exists within a securitized society relies on thinking about the future via data averages and virtualities. What is the likelihood, for example, of some individual committing a crime? Stringently as a matter of biopower (but, let's be honest, everything is), the kind of security that Foucault explains differs from the disciplinarian security state proposed by Hobbes, for instance, in the way its mechanisms interact with each other. As Foucault (1995) writes, "You have a series of complex edifices in which, of course, the techniques themselves change and are perfected, or anyway become more complicated, but in which what above all changes is the dominant characteristic, or more exactly, the system of correlation between juridico-legal mechanisms, disciplinary mechanisms, and mechanisms of security."

The statistical data on which security relies is a positivistic prediction of the future — a horoscope of securitized possibilities through which governance is enacted. Both traditional security assemblages and consumer friendly technologies that focus on the face as an object (and

here, of course, the face can refer to the literal face, or the social technology) in motion do so in an attempt to discern future behaviors.

Prior to this dissertation, I became interested in such technologies by reading and talking with colleagues about programs like SPOT (Screening Passengers for Observation Techniques), and the Department of Homeland Security's FAST (Future Attribute Screening Technology. SPOT trained airport security personnel to focus on micro-expressions, while FAST, originally referred to as Project Hostile Intent, and AVATAR's predecessor, was an assemblage of cameras lasers, and infrared sensors that attempted to find "unknown terrorists."

Lauren Wilcox, in *Bodies in Violence* (2015), explores how the usage of technologies like these represents a weird irony in the temporalities of security. Namely, that, while their aim may be to look into the future, bodies are thus presumed to be "fixed and unchanging as objects of scientific gaze (2015)." Bodies are not only knowable, but readable; they are non-temporal objects through which the future can be read in numbers, facial ticks, heat differentials, and eye movements.

The point where present, unmovable body, and future flows in security meet is the affect that these technologies are assumed to capture via an expressed embodiment; unconscious smiles, frowns, temperature changes and even linguistic habits are indicative of a kind of datafied intensity in the body, present statistics and likelihoods for the future events of that body. Technologies of so-called "affective computing," which seek to discern what makes hearts race or skin flush, are indicative of the increasing intimacy with which securitized logics are attempting to solidify an uncertain future. They work through the assumed "static" medium of the body, channeling the computational logic that Wendy Chun (2011) discusses in *Programmed Memories*, where command equals control. The space in between — in this case, experienced

time and contingencies — doesn't exist in the context of securitized governance and logics. This interaction between embodiment and the digital is not reserved to the security milieu, as we've discussed.

The consciousness of global collectivity (via mass connectivity) unfolds with the same kind of temporal flow of the products of computational and programming industries, thus positing an experience of time that is both embodied and mediated via the technologies we imbibe. Bernard Stiegler (1998) introduces the industrial temporal object in *Disorientation.* An object is temporal, he argues, when its flow "coincides with the stream of consciousness of which it is the object." In *Technics and Time,* Stiegler (1998) examines this industrial temporal object to follow the ways in which these objects work to prime consciousness and subjectivity via some "anonymous elsewhere." With an increased amount of time in front of the interface comes the industrial temporalization of consciousness. Stiegler writes the convergence of "industrial logistics (informatics), transmission (telecommunications), and the symbolic (audiovisual) … integrates the functions of technological, industrial, and capitalistic mnemotechnical systems into the technical systems producing material goods … in turn subordinating the entire worlds of culture, knowledge, and the mind, along with artistic creation and advanced research and instruction, to the imperatives of development and the market."

Stiegler's concept of temporal objects is a means through which to think through connectivity, security, and surveillance societies, while conceptualizing the wonky temporalities of the process of embodiment as it experiences the digital. In thinking through the temporality of connectivity, treating computation as an industrial temporal object adds a technical (and temporal) dimension to the way Brian Massumi considers how affect is primed across populations. Using post-9/11 terror alert spectrums, Massumi (2005) shows that centralized

informatics can work as a kind of "distributed neuronal network registering en masse quantum shifts" in the affective, ontological experiences of a population. Thus, not only do programmatic objects like these create population-wide shifts in affect, they can work to program how consciousness and temporality are experienced, creating embodied subjectivity that is primed to a geopolitical notion of affect and twitchiness and to a techno-contingent logic (and experience) of time.

That experience is one of constant attention — connectivity, in the vein of Stiegler's "immediate reception," which not only makes everything into an event, but relies on *constant* liveliness. Crary, again in his work on sleep and attention (2013), works through how the modern network supersedes human demarcated time with the digital, conscripting life into "duration without breaks" defined via continuous functioning so that time no longer passes beyond the numbers on a clock. Social identity has been reorganized, he suggests, to conform with the uninterrupted operation of markets, information networks, and other systems. By focusing on a specific embodied experience (sleep), Crary (2013) presents a valid critique of Stiegler, suggesting that more important than the capturing of attention via some kind of "delimited object" are the ways in which attention is remade into repetitive operations and responses that involve looking and listening. Put another way, it is less the homogeneity of media that perpetuates the alienated modern subject and more the "larger … compulsory arrangements within which these elements … are consumed." It is these large, compulsory arrangements – these systems of extraction, of attention, of spectacle and programming, of once in a while, a metal tube strung across the bottom of the ocean, that the embodied subject is always already a part of.

The embodiment Crary brings into his conceptions of time and attention is one that highlights the subjectifying tendencies of increasingly intimate technologies. The screen that we stare at — and that we give our attention to — increasingly stares back. Thus, there is a dual visibility at work, a dual kind of attention that forms the subject not only via technical definitions of embodied movement (facial expressions as geometric points; corporate designed avatars that represent a specific formation of racialized American femininity; deepfaked Presidents and their comedians) but also via technical definitions of experience and flow.

Relatedly, and another worthwhile element of Stiegler's work with cinema, is to treat the face, the body, itself as a kind of spectacle; a temporal object with political and securitized consequences as it affects the ability of certain assemblages to retain control and authority. While cinema (through which Stiegler posits his arguments) is inadequate as a model of media in encompassing the ways that modern technology facilitates the global transmission of data without the necessity for human intervention or perception, it does help in understanding how the face is made, especially through technologies that then augment temporalities, again independent of human experience, to identify lies, to find dangerous bodies, to codify intent, and to capture affect.

Chapter Two: The Securitized Face: Expressions and Subjectification at the Border

In mid-2018, AVATAR, or the Automated Virtual Agent for Truth Assessments in Real Time, was licensed and prepped for commercial scaling via Tech Launch Arizona, the University of Arizona office responsible for commercializing inventions from Arizona university research, and the university's spinoff start-up Discern Science International, Inc. (Tumarkin 2018). Originally a product of the Borders Research Project, and funded by the United States Department of Defense, National Science Foundation, FRONTEX, and the Department of Homeland Security, AVATAR was touted as "deception detection" technology, meant to streamline the border crossing process via automated algorithmic questioning. It worked like this: An on-screen avatar (Caucasian; male) housed in an "all-in-one" kiosk posed questions while a bevy of biometric software measured voice, body temperature, eyes and recorded facial expressions. This information was then routed through an algorithm that, ostensibly, worked to detect deception. Within thirty seconds to a minute, border agents would be given a post-interview conclusion from the data collected by the avatar, key in deciding whether interviewees had been attempting to deceive the kiosk, and thus, would be allowed to cross the border or kept for further questioning.

Using AVATAR as its point of entry, this chapter attempts to complicate the notion of the modern and future "e-border" and extend the thinking already done to consider AVATAR not merely as a space/event in which the body is dissected (Amoore, et al. 2013) at the hands of some proxy sovereign, but as one through which biometric technologies *facialize* the biometric-semiotic encounter. AVATAR is not unique, nor is its dissemination across border spaces an inevitability, but as a device it is an articulation of the programmatic logics of the security assemblages it exists within. As an Embodied Conversational Agent (or, ECA) (Nunamaker

2011), a device that uses AI and biometrics to digitally represent human *interaction*, AVATAR gives fruition to the guiding *logos* of preemption at the border while also representing the pervasively intimate relationship between the embodied/facialized subject and the face of authority. That is, devices like AVATAR exist within a space in which the performance of the body (and, more specifically, the performance of the face) becomes securitized. AVATAR's effectiveness as an ECA relies on an explicitly facialized relationship between subject and machine. Thus, the primacy of the face in this acutely securitized environment begs the question: Why does security need a face? And, when it gets one, what does it do with it?

In one sense, AVATAR was (and still is) part of a larger push to automate the border space. With international funding by agencies responsible for border security and management, the project was exemplary of the so-called "e-border" concept (FRONTEX 2016; MacLeod 2011) in which biometric and automated systems are used to make the border crossing process more "secure." Prior analyses of AVATAR-like systems have focused on the implications of this technology within the nodal logistics of modern security (see, Muller 2015). As an alleged technological solution to the post-9/11 problematics of insecure borders and securitized migration policies, AVATAR and systems like it can be seen as indicative of emerging global norms of border-security management. In this system, the logic of preemption acts as a guiding principle for commercial, private, military, and technological actions. Uncertain futures – the possibility of low-probability, high consequences events (Amoore 2013) – are mapped and acted upon as concrete possibilities. Risk, and the measurement thereof, becomes the operating condition for the border, and in this space, embodied assumptions about danger, otherness, and insecurity are condensed into a form of proxy sovereignty dependent on private consulting, software, and biometrics engineering (Amoore 2016, 6).

My focus is not on AVATAR's success or failure as it was, is, or will be, implemented at borders. Failure does not undo the intent behind the involved process that has gone into AVATAR's development in the first place. And the reality of technical failure and success is both produced by, and produces, existing cultural frameworks and ideologies. So while the implementation of biometric technologies at the border is a necessary and important analysis to take up, especially considering the risk to targeted populations a false positive represents (Gallagher, & Jona 2019), this chapter is instead committed to understanding the *desire* for a particular type of security symptomized by AVATAR's existence; the *desire* for a face, as it is simultaneously captured and simulated via automated technologies. I am concerned with the design, material supports, and operational principles of ECAs in general (Bousquet 2018, 17), and what these devices say about the need for modern security assemblages to not just identify but *know what a person is*— past, present, and future (Pugliese 2010).

With that in mind, this chapter proceeds in three parts. First, I work to place AVATAR within a genealogy of biometric and social technologies meant to identify and authenticate. By unpacking the logics of identification and authentication within the context of contemporary security practices and their predecessors, I attempt to situate AVATAR within a milieu of racializing and dissecting technologies as well as racialization and dissection *as* technologies. Following David Theo Goldberg, my use of the term racialization here is meant to signal those moments and logics that reify borders along racial lines and where the outcome is often discriminatory (Goldberg 2002, 12). I argue that AVATAR makes concrete a kind of algorithmic physiognomy or phrenology – an automated racialization of the individual via their facial expressions and features. The face, as both simulated and captured within the AVATAR assemblage, builds on an idea of nationality and sovereignty that emerged in tandem with new

forms of scientific racism and nationalism in the 19th century. This "national character" acts as a linchpin through which to understand how the performance of inclusion and exclusion occur at the border.

Next, I consider the implications of AVATAR, and technologies like it, as a framework for deception detection. As a technology, expression tracking is reliant on a number of algorithmic logics that make public expression via the face a matter of performative embodiment. This performativity is contingent on very specific conceptions of deception, and how that deception is shown or obfuscated on the face. In attempting to understand how the face and its expressions can be securitized via these logics, I consider the work of Paul Ekman and Interpersonal Deception Theory, or IDT (See Ekman 1971; Ekman 1980; Ekman 1999). Contemporary expressions tracking algorithms retain key technical perimeters from this school of thought that work to create the conditions through which faces are treated as objects — standardized, dissected, securitized.

Finally, in the last section I consider AVATAR as an interpellation (Althusser 2014) of the mobile embodied subject. The ECA, as a genre of device, attempts to emulate human interaction via the simulation of expression, affect, and emotion via a digital avatar. It is through this interface that the face of authority — in AVATAR's case: white, male, heteronormative (Wehner 2016) — becomes visible, encapsulating those interviewed within a task-based regime of performative sovereignty and subjection. It is through this simulation, I argue, that the post-9/11 commitment to securitization of the face becomes more than just a matter of digital dissection (Amoore 2013) or surveillance, but of biometric discipline and control. The emulation of authentic human interaction via digital avatar, in contrast to the interviewee's assumed "deception," treats AVATAR as an articulation of discipline as it is both captured and produced,

making possible a subject that works to recognize themselves in the face of a digital stand-in for the state. This face *acts* on its environment; it is imbued with cultural mythologies that constitute the authoritative, the trustworthy, the composed and informative, even as its designation as an automated biometric assemblage claims objectivity and sterility.

Thus the question of *why* security needs a face, I argue, is a matter of machinic faciality. Taking from Deleuze and Guattari (1987; 2010), I attempt to complicate the logics that go in to making AVATAR and face-based deception detection a standardized solution to insecurity. The face, Guattari argues, works to "delimit what is legitimate from what is not. Faciality subjects the face to the broadest significant consensus, thus introducing diagrammatic processes of control: "*There are certain heads that do not pass in the system. It is necessary to hide them, cut them off, make them over, or better yet transform them from the inside (*Guattari 2010, 75 – 76)."

AVATAR does not only capture the face and its expressions as concrete data-objects to be dissected, but also presents an image of *acceptable* faces that make *acceptable* expressions as it does so. Biometric assemblages like AVATAR, which actuate state-subject relations via programmed and programmatic embodiment, are not merely technologies that exist within a space of automated security, but also signal a state-level interest in securitized faciality. AVATAR is a technical and cultural machine (Latour 1987), a device that helps in explicating the work that goes into performing sovereignty, identity, and authentication at the border by government agencies, technologies, epistemologies, and subjects.

It was designed, as such, to anticipate more generalized security logics. Taking note from other scholars working on the redistribution and expansion of the border (Bourne, Johnson & Lisle 2015), I consider AVATAR as indicative of this security logic not just through its technical specifications, but through the "scientific and technological imaginaries" that went into its

development (Parker and Vaughan-Williams 2012; Salter 2012). Devices used at the border, ECA among them, are machinic concretions — conceived and produced to varying levels of technical success and/or failure to fulfil some mandated function within a wider security assemblage (Bousquet 17). This function is a political act, a statement on how the border is performed and maintained, and how this statement is conceived through larger desires for a specific type of security. I see AVATAR as Simone Weil suggests, by considering not just the ends pursued by its implementation within the liminal space of the border, but as the "consequences necessarily implied by the working out of the means employed (Weil 1999: 173)."

Biometric Identification and Authentication: Placing AVATAR

Biometric technology is most commonly used for the verification and authentication of identity (Muller 2010, 32). Biometrics, from their inception, are a technology of capture, predicated on using an image to curtail deception of the subject and thus, turning corporeality into "evidentiary data inscribed within regimes of truth." Biometric logics, as Joseph Pugliese suggests, always already conflate *who* you are with *what* you are, which in itself necessitates an inter-related and complex relationship between the act of identification to that of authentication (Pugliese 2010: 2 – 3). Within this identifying and authenticating regime, AVATAR actuates a by now familiar subject-state relationship in which biometric technologies maintain and perform proxy sovereignty. AVATAR relies on "automated" human-to-human conversation simulation and simultaneous expression tracking in a bid to capture deception as a form of *intent.* This extends the work of biometric identification into an affective-temporal space not yet considered.

That is, the dissection of the body at the border is not, primarily, one of surveillance but of *projection* (Amoore, et al. 2013). The current body — an unchanging, dissected "snapshot" of the mobile traveler — is tasked, in this space, with confessing the sins of its future to an automated confessional (Salter 2007). AVATAR, however, encodes that projection within a biometric program intended to capture affect. Whereas other biometric technologies focus on physiological manifestations of body stressors (such as increased pulse, temperature, gait, etc.), the AVATAR system's emphasis on the face and its expressions suggests an extension of securitization into the affective realm. With AVATAR, a facial expression made at one point in time is treated as a risk assessment for the future. AVATAR, then, suggests a *temporal* and *affective* shift in what is considered possible to be seen by the visual, automated gaze. This extension, however, owes its novelty to a history of biometric (and pre-biometric) identification and authentication in the Western security imagination.

***Identification/Authentication: A Genealogy of Biometrics*.** Contemporary security practices, seeking to fix identity at the border, are an evolution of efforts in aesthetics, criminology, and medicine to mine the body for possible certainties, and thus, reveal clues to an as-of-yet experienced future (Amoore et al. 2013, 447). The search to identify a suspect via deception, then, is an integral part of the biometric assemblage, and one that rests on the simple, albeit contradictory logic that individuating signatures (gait, expression, fingers) must be reproducible and to some extent standardized while still appearing unique in order to maintain any kind of identifying function (Pugliese 2010, 25). Everyone must have fingerprints to scan, but those fingerprints should be unique to them; everyone must walk, but must walk a certain way lest they be labeled deviant; everyone must have a unique and *identifiable* face, but the way

in which that face moves must fit into a pre-coded and scanned database. And, of course, each movement must be unique to a single, *universal* emotional-affective state of mind.

These movements themselves are, additionally, encoded within the technologies of race, nationalism, gender, and ableism that called for their classification. Early processes of identification, such as Petrus Camper's *Treatise (1794),* a series of illustrations showing the "national features" of individuals from "different countries and periods of life," established racial codes and logics that worked to articulate the difference between the civilized European and the "ape-like" African (1794, 84). Camper's work is a piece of racialized aesthetics, founded on the idea of the European body as the normative standard, as the ideal, a template white body that operates through the violence of negation and exclusion.

This same aesthetics informed the usage of phrenology and physiognomy as indicators of "authentic nationality" in the 19th century. Phrenology, the "identification of basic brain functions and their manifestations in cranial features" (Schlag 1997, 1), and physiognomy, the "linking of facial features to character," incorporated (and still do incorporate) various folk beliefs about human development and morality into mildly more scientific jargon, working to shelter and legitimize "existing beliefs by recasting them in a scientific mold (ibid., 9)." Conferences, symposia, and scholarly journals provided fertile ground for the deconstruction of the face and skull as a matter of not only identification, but of *identity*. Phrenology and physiognomy weren't just intended as methods to identify individuals, but to *know* those individuals; to be able to "read" embodiment as symptomatic of character, morality, intent, and intelligence. They incorporated common social assumptions about human development and morality into mildly more scientific jargon, sheltering and legitimizing "existing beliefs by recasting them in a scientific mold (Schlag 1997, 9)." They were sciences of *authentication,*

creating a "scientific" language through which to apply and justify social stigmas, stereotypes, and prejudices via an apparently objective lens of measurement.

As well, studies linking facial expression and facial characteristics to illness (Boulogne 2006) and criminality (Bertillion 1901) relied on the assumed objectivity of the newly widely available photograph to posit the face's role in identification as a matter of scientific documentation, rather than culturally specific interpretation. Unsurprisingly, many of the methods of identification and authentication supported by phrenology and physiognomy are explicitly racist and gendered, ascribing inferior physiological capacities to non-white, non-male faces (Schlag 1997, 10). And, via the same kind of normative judgement's eschewed by Camper's *Treatise,* they promote the idea of a generalized national physiognomy and character type. Johann Casper Lavater, writing in 1840, argued that "that there is a national physiognomy, as well as a national character, is undeniable (339)." This "national character," conceptualized in popular discourse during a time of increasing globalization and ontological insecurity, exists as an embodied truth discerned via racialized and gendered readings of the face.

By extension, the idea of nationhood, and thus, the exercise of sovereignty that emerged in the latter half of the 19th century drew upon physiognomic and phrenological coding of the face as a site of truth to produce legitimations of nationalism and colonialism, treated as a form of authentic identification (Twine 2002, 74). The face was —as Francis Galton, a leading voice in the eugenics movement, considered — a way to "bring into *evidence* all the traits in which there is agreement, and to leave but a ghost of a trace of individual peculiarities (Galton 1883, 10)." Physiognomic discourse, then, was a means of entrenching hegemonic conceptions of character, nationality, gender, and race via their legitimization through the "truth" of the face as a method of identification, with skull shape (phrenology) and facial traits (physiognomy) both

being treated as a means of classification and "objective" judgement. Citizenship and nationality becomes, through these practices, a matter of conscious deception and unconscious, embodied authentication.

Deception Machine. AVATAR in Practice

Deception. AVATAR's integration into any modern e-border milieu relies on these same evidentiary logics, deployed in the name of security, meant to "cast the net as widely as possible [to] identify suitable enemies (Muller 2010, 118)." Indeed, the promise of biometric data at the border is to see what is *really* there (Hall 2017, 501). Or rather, to see what is *really* there with more efficacy, speed, and perceived objectivity than any individual (human) border agent. Seeing what is really there, in this context, becomes the practice of superseding the deceptive subject via the digital dissection of an authentic "unconscious" body that does not change or decay. The idea of the inauthentic subject versus the authentic body, applied as it is to biometric systems, can be credited at least partially to the work of Paul Ekman and his colleagues (Ekman 1971; Ekman, 1980; Ekman, 1999) and their research into interpersonal deception theory, or IDT. This school of thought, especially in the mid-20th century, worked to coin the idea of the micro-expression, the idea of emotional leakage and, eventually, the FACS, or the Facial Action Coding System, as a means of uncovering deception using the body, and, especially, the face (Hall 2015).

Ekman's initial research into emotion relies on the study of only right-handed Caucasian women to conclude that spontaneous expressions are universal to eight basic emotions (Ekman 1980). Meanwhile, his argument that emotional-affective expression remains universal across culture – a technical assumption integral to most biometric systems tasked with capturing and

analyzing emotion via facial expression – is based on an anthropological study of the members of the Fore tribe of Papua New Guinea, chosen because of their minimal interaction with "literate" Western cultures (Ekman 1971). In this study, individuals were asked to react after being told a story correlating to a specific emotion ("Sadness: His (her) child (mother) has died, and he (she) feels very sad" (Ekman 1971, 126). Ekman, consulting with Margaret Mead, Gregory Bateson, Edward Hall, and Ray Birdwhitsell, tempered this universal claim by acknowledging the cultural implications of performativity, suggesting that while in private people "use the same innate expressions, they have learned from their cultures to manage those expressions differently when in public (Hall, 215)."

By postulating that standard emotions correlate with standard expressions, and that these standardized emotional affective reactions were *universal* across cultures, Ekman and the IDT school laid the theoretical foundations for a system of automated expression recognition, easily mechanized for the purpose of perceiving alleged deception. Ekman's Facial Action Coding System (FACS), especially, is used as the expression cipher *de rigor*. The system works by treating affective responses as a set of standardized symptoms; individual muscular twitches are codified and then reorganized into algorithmic points, and subsequent mapping, of the face. Used by law enforcement in interrogation (Matsumoto 2014), by advertisement companies seeking consumer feedback (Qualtrics, Protobrand, Kantar Added Value), by academics conducting psychological and behavioral research (iMotions) technologies using software encoded with FACS capture logic have been used to seek out and capture "authentic" pre-linguistic reactions to external stimuli. FACS has codified not just a specific, historically contingent materiality of affect, but also works to entrench the conception of affect as separate from emotion within a space of algorithmic mediation. The idea of the authentic expression – a raw collection of

twitches, muscular stretches, and epidermal creases – ignores the subject for the object, sidestepping conscious participation on the part of a possible criminal, consumer, or research volunteer to get to the somatics of the pre-sociolinguistic impossibility of deception. The body tells the truth through affect while the subject lies through emotion.

As mentioned, the FACS system works by isolating the musculature involved in specific expressions as "action units." Within this programmatic space, the smirk, for instance, is differentiated from the smile via the symmetry or asymmetry of the zygomatic major muscle, or AU12 (Senechal 2013). Kelly Gates explains how FACS draws conclusions from the faces it analyzes: "[Accuracy] is defined not in terms of the correspondence between the system and the person whose face is being analyzed (or the full range of ways a facial expression might be interpreted), but in terms of the system's internal agreement – that is, whether the classification system consistently agrees with itself (Gates 2011, 171)." Far from neutral, the true power of FACS technologies, and by extension, expression tracking automation, is when this form of "accuracy" in turn gets pushed back out onto faces, coming to define what facial expressions mean and how they work, whether in the liminal space of the airport, or in the wider securitized border network.

FACS creates the conditions through which new meanings of the face are made possible. It maps out the "surface movements, temporal dimensions, and intensities of the face with the aim of interpreting the interior state of the person, claiming that those surface movements… provide directed *unmediated* access [to the individual] (Gates 2011, 174)." Expression tracking technologies rely heavily on FACS and systems like it to discern affect from expression — indeed, the research group behind AVATAR cites Ekman's work as integral to their design of device-specific expression capture systems (Nunamaker 2011). AVATAR'S predecessor, known

as SPECIES (Special Purposes Embodied Conversational Intelligence with Environmental Sensors) was developed via three motivating axioms to which FACs technology was applied: "people deceive, humans are poor lie detectors, and there are many circumstances when credibility must be rapidly and accurately determined (Nunamaker 2011, 18)." This so-called "credibility" is defined via, of course, affect as shown via facial expression — the leakage, as such, of an internal emotional state through an external physiological expression.

Automating the detection of deception, however, doesn't merely require highly specific technologies and definitions of embodiment. It also requires the re-definition of deception as a form of embodiment itself, and into something that can be standardized for the purposes of authentication. Indeed, while FACS and other facial coding systems are able to isolate expressions, automating deception detection (still a relatively new technology; see: Twyman 2012) is difficult because *there is currently no proven single behavior or physiological state that correlates, directly and universally, with the state of deception itself* (DePaulo 2003). Of course, leakage theory posits that the face shows fear, anger, or contempt during deception (Ekman 1969), research into ECAs like AVATAR attempt to further measure authenticity and credibility by not only assessing facial movement, but the *lack thereof*: "A major drawback when relying on facial emotions as inputs for risk assessment systems is how well people can control their emotional displays (Pentland et al 2017, 976)." Even as expression becomes integral to the securitization of the body, so too does its lack. Facial rigidity and emotional neutralization – performative behaviors, perhaps, in response to the border interrogation process – become risk factors.

Performativity at the border takes on a number of ontological pathways. Here, however, the social construction and maintenance of the border (Wonders 2006, 64) is one in which the

border exists as both a performance and the lack thereof. That is, the performativity of the body becomes just as capable of malintent or deception, just as dangerous as the leakage (or, *lack* of performativity) of the body: A neutral expression, rigid shoulders, straight spine, and little vocal inflection become just as suspicious during the border interrogation process as facial representations of anxiety, fear, or contempt (Salter 2007b). The possibility of facial rigidity measurement and analysis suggests that face-based deception detection is more a matter of self-authentication on the part of e-border algorithms than the documentation of authenticity. In addition, the logic behind the measurement of *both* embodied performativity the *lack* of embodied performativity (via the same body) at the border suggests that the question of deception is performative itself. Just as sovereignty is performed and reconstituted at the border through continuous decisions about who is a citizen and who is not, the ability to define deception (accurately, rapidly, and without the infallibility of human discretion) contains and disciplines the mobile traveler, putting the onus of proving oneself as a non-risk on the individual; everyone and anyone becomes deceptive until they have proven they can "perform" within the parameters of the sovereign program. Until one has proven that they are a face that fits into the system (Guattari 2010, 75).

It is as necessary to produce evidence of deception to sovereign powers at the border as it is to produce truth, thereby authenticating the safe from the risky, the deviant from the normal, the us from the them. The automated border examination, structured as it is around the embodied, facially specific detection of deception, and therefore, malintent, is an encoded space of algorithmic logic, holding its subjects within what Michel Foucault considers a mechanism of objectification (1978, 187), through which deception becomes the means by which individuals

define themselves as privy to the sovereignty of the nation-state at whose border they are examined, as well as the logics of the machine by which they become data.

While AVATAR consists of an assemblage of sensors aside from expression tracking algorithms, these biometric scanners are intended for the same purpose: to automate the coding of deception upon the body at the border. The securitization of the face via expression tracking, built upon the anthropological and psychological research as discussed above, highlights the automation of biometric systems at the border as both objectification and subjectification. This institutional and political commitment to the ideal of automatically detected deception makes possible a space in which sovereign technologies work to render visible the body as both object and subject; captured not just as a collection of data points, but as a standardized formulation of national character defined from a contingent definition of the lying body (face).

Faciality

Of course, the face and its expressions have long been treated as telling of some "internal passion" (Zevnik 2016; Boulogne 2006). In his studies of hysteria in the late 19th century, French neurologist Jean-Martin Charcot photographed his patients' faces as he sought to analyze the symptoms of hysteria. Through these portraits, Charcot hoped to provide diagnoses for future episodes of hysteria through the observation of his patients as they exhibited what were then considered symptoms of the condition. Ticks, twitches, smiles, frowns, and shudders became symptomatic, a medical narrative that allowed hysteria to be constructed within the constraints of facial characterization. Put another way, Charcot believed hysteria could be characterized by the face; a physiological sign of psychological origin, as well as visual evidence of hysteria as a kind of alterity or deviation from the norm.

Charcot's work was not merely passive documentation of physiological phenomena. His initial diagnoses of hysteria were proven limited enough that it became necessary to "provoke" an exhibition of particular facial expressions through electrical stimulation. His record of hysteria in patients was less about the identification of symptoms in the wild and more about the authentication of his thesis; that facial characteristics could, standardized, provide an inroads into diagnosing what was seen as an internal problem. Like Charcot, Guillaume-Benjamin Duchenne, a fellow neurologist, also sought to provide stimulated expressions for medical symptomization. *The Mechanism of Human Facial Expression*, first published in 1862, consists of a series of portraits in which Duchenne is seen holding metallic rods to various parts of a subject's face, their expressions morphed into gestalt characterizations — Lady Macbeth, contemplating "unknown cruelties," The Nun; The Expression of the Damned — by electrical impulses (Boulogne 2006). These simulated expressions evolved from a physical diagnosis to an encapsulation of the subject photographed within a form of facialized subjectivity, reliant on a sense of the face as a physical and aesthetic objected imbued with medical (and insecure) data.

Charcot and Duchenne believed their photographs to be a representation of a scientific reality (Zevnik 2016, 129). Instead, they merely authenticated racialized, gendered, and classed assumptions already held by their progeners via the supposed objective technology of medical photography. Implicit within this logic was the desire to *see* hysteria within the expression and the face, to authenticate the program itself (in this case, an archive of expressions diagnosing an alleged mental health issue) using provoked (electrically stimulated) actions to do so. Data and algorithmic automation at the e-border is another attempt at this form of vision. Finding a causative relationship between expression and hysteria constitutes a subject within logics of medicalized embodiment, just as finding a causative relationship between expression and

deception subjects, and subjectifies, individuals to a form of faciality that is machinic and material, based on an ideation of securitized — leaky, full of actionable intelligence — embodiment.

The face exhibits deception within modern security assemblages, and expression tracking technologies work to create the conditions through which this is possible. Indeed, this connection between medical symptomizing and modern facial security is not merely a theoretical one. When Ekman and associates began work on FACS in the late 1970s, they turned to Charcot and Duchenne for inspiration, with Ekman electrically stimulating his own facial muscles to measure the movements that constitute expressions via muscle specific action units (Ekman 2007). Expression tracking is not merely a tool of criminology or security, but also a technology that symptomizes the face via outside manipulation and interpretation. Systems reliant on the FACS model – standardizing the face as a collection of geometrically defined points – require a medicalized, racialized, and gendered conception of the face as a narrative, as well as a relational space primed to define the subject only as authentic as their body betrays. Indeed, any digital dissection and subsequent othering within the border interrogation process occurs not within the psychoanalytical gaze of the other, but within the machinic logics of the algorithm. ECAs, as an articulation of the desire for an ideally automated border, are representative of a larger, predominantly Western security apparatus, but they also highlight the role that machine vision and posthuman modes of perception play into this liminal space.

ECAs like AVATAR make possible a reflection of the subject – the interviewee, or person at the border, or patient being documented — through inhuman eyes. The liminal space of the airport, as a border, is an anxious space; it represents the intersection of mobility and identity. It is within this space that Mark Salter identifies the anxious, self-disclosing citizen — a subject

conditioned "by the Christian notion of continual, exhaustive confession in the face of the state apparatus" (Salter 2007a). Along with this confessionary anxiety, AVATAR presents a distinctly phenomenological sense of posthuman eeriness through a face-to-simulation encounter, a machinic 'othering' through which individuals are made aware of themselves as measured and seen, judged against some unknown standard. Through which the border becomes not just a space where individuals "confess one's crimes, one's sins, one's thoughts and desires, one's illnesses and troubles" (Foucault 1978, 59), but where one encounters themselves divested of anything save for their biological operations. *Bios* is sloughed off, and the subject is understood as a function of their parts, where the face becomes merely an object to look at and make sense of; to symptomize. This object, this face, is identified and authenticated via its relationship to a database of other faces. Faciality, and the act of facialization, become a politics. Indeed, as Giles Deleuze and Felix Guattari suggest, faces constantly over-determine identity: "…when the body, head included, has been decoded and has to be overcoded by something we shall call the Face… if the head and its elements are facalized, the entire body… also comes to be facialized" (Deleuze and Guattari 1987, 170).

The face, they continue, is "not universal" (ibid., 176). It is not something that everyone has, nor is it a natural form of corporeality. The face, instead, is part of a political system that proves it to be useful, making it submit to particular regimes of power. The politics that make the face is a politics that treats the person as an object, pinning them down to be laid bare, made available, to be seen by any number of state or private apparati, be they part of a bureaucracy or administration or border crossing point (Edkins 2015, 7).

Faciality only works as much as it exists within these systems, through which facialities of reference are adjusted, maintained, and legitimized. Guattari extends this thinking by

suggesting that, "for a *deviant* faciality, crossing certain thresholds has become a veritable predestination to an assumption of responsibility through specialized equipment. All the phenomena of communication and exchange are dependent on the laws and jurisprudence governing the dominant faciality" (Guattari 2011, 95). Some faces don't fit into the system, and when no method of classification, or equipment can situate, for instance, a frown or twitch or smile, dominant facility itself explains away the deviation. ECA and adjacent technologies represent the digitalization and automation of deception detection via a physiognomic form of faciality, and their treatment as 'objective' solutions to the border is emblematic of a security logic that desires for a fully knowable, seeable, and containable, national "character."

The Face of Authority: Embodied Conversational Agents and Interfacial Interpellation

Prototypical Whiteness. AVATAR is a technology of corporeal fetishism, a way to "simplify and condense complex relationships… into singular digital maps of the body… free from the alleged 'failures' of culture (Wilcox 2017, 15). But ECAs in general, and expression tracking models specifically, rely on this longer history of gendered and racial means of differentiating bodies and cultures: indeed, it is impossible to separate machine from culture. AVATAR is an example of the ways in which technologies acts on, and are acted upon by, culture. The research that went into the development of Ekman's FACS and, subsequently, automated expression tracking systems , is not free of cultural assumptions about race, gender, and nationality. Ekman's work on exterior expressions coinciding with interior emotion exists due to research conducted via the faces of thirty-five Caucasian-American right-handed women, an easily standardized demographic chosen because prior studies showed "some differences in facial encoding associated with gender (Ekman 1980, 1126)." Similarly, the "proof" of the

universal facial expression relies on a colonial literate/preliterate binary applied to the Fore people of Papua New Guinea for the purpose of proving that, even without the effect of Western popular media, facial occurrences are the same if you "ignore" the performance of culture (Ekman 1971). What this conceptualization fails to grapple with is its implicit reliance on a conceptualization of prototypical whiteness as an unspoken standard of comparison. Joseph Pugliese highlights the social Darwinism inherent to this racial hierarchy: the notion of certain racialized and gendered bodies – racialized and gendered facial expressions and structures – only makes sense when male whiteness provides the standards against which these groups are compared (Pugliese 2015, 8). The Caucasian women recorded during Ekman's work on facial expressions, as well as the Fore people interviewed during his work on cultural expression, are considered as deviations to the emotionally neutral white male (Ekman 1980) and/or the *over-cultured* white male (Ekman 1971).

In AVATAR's design imperative the idea of prototypical whiteness is, perhaps, made literal: expression tracking algorithms, formulated as a result of research that implicitly *others*, track and code the face for deception, just as a (white, male) face meant to act as a "standard" of behavior exists as a point of authority and control.

Interpellation. With ECAs, the performance of deception as a matter of objectification exists *alongside* the performance of subjectification. The simulated "conversational agent" in this context is designed for the purpose of treating "human interaction [as the] main control component" in the border authority and targeted mobile traveler relationship (Nunamaker 2011). Where objectification treats the individual as the *object* through which power is applied, I take my definition of subjectification via Louis Althusser's infamous bit of political theatre describing the act of interpellation. That is, that subjects recognize themselves via the conditions imposed

upon them, becoming implicit in their own domination (Althusser 2014). As Foucault suggests, power in this sense is both *subjection*, or the individual submitting to domination, as well as *subjectification*, when the individual, subjected, constructs themselves through this identification and relationship to power (Foucault 1982). Individuals are always-already subjects, interpellated by ideologies built into the media (and mediums) they experience. AVATAR and machines like it are ideological apparatuses, and while interacting with it, individuals are positioned to identify themselves with and through the face they see on screen. Here, the "face" of the interface is somewhat literal. AVATAR acts as a construction of an image of the state, and it is through this interface that subjectification occurs. The object – the face of the traveler – becomes the subject through interaction with an interface that presents a particular definition (and face) of authority as hegemonic ideology. The individual is presented with an *ideal*, a face par excellence, just as they participate in a process that, as this chapter has discussed, considers their face, and its actions (or lack thereof) wanting.

Interfaces like AVATAR represent a kind of institutional faith in a number of theories, or perhaps, assumptions, on affective computing. Key among them is that in automating the border interrogation process, more information can be gathered when human subjects engage with and respond to the gestures and statements made by an ECA, then when they are merely given a list of questions to answer (Pentland 2017, 21). AVATAR is an emotive interface; when embodied agents react to human subjects "appropriately" (Eastwood 2014, 764) emotional responses to cues can then be recorded and measured as a risk or non-risk. Thus, emotion-oriented border technologies require programmers and designers to consider both facial capture and facial *simulation*. This simulation requires that the face be understood not just as something to be captured and measured for the purpose of revealing deception or malintent, but also that it be

constructed digitally to perform strategically. Identifying emotion in and from synthetic faces is more difficult than identifying emotion in another human, however — in order to be effective, expressions made by simulated agents need to be performed dynamically so that interviewees "speak longer and say more (Pentland 2017, 22)." And, as was proposed with AVATAR, photorealistic agents need to be "completely lifelike," with natural expressions and mannerisms, or else they are preferred less than a disembodied voice (ibid).

The screen interface is AVATAR's primary means of influencing the environment around it — the signals and messages it displays via the expressions it simulates affect the performance of its interviewee, as well as the interviewee's recognition of themselves as a subject through the eyes of the ECA. As such, the parameters of *how* the interface affects its user depends on a few primary dimensions. Notably, voice and appearance.

Interaction with AVATAR is based on a table of dependent gendered and racialized social constructs around power, composure, trustworthiness, expertise, and likeability, that are then used to rate how these semantics affect user perception. During development, AVATAR'S appearance was manipulated to show different "demeanors, genders, ethnicities, hair colors, clothing, hairstyles and face structures," all of which were meant to actuate the performative politics of the border space – theoretically, wherever that border may be. Indeed, larger, male-gendered avatars were said to be perceived as more dominant than female-gendered avatars (Pentland 2017, 23); perceptions of high expertise, worthiness, and credibility, shown via clothing, face structure, skin color, or other features, ostensibly made participants respond to the kiosk more seriously (ibid., 28), and intimidation via a gendered-racialized- avatar demeanor maybe have caused "those harboring malicious intent" to reveal contempt, anger, or fear to a greater extent than those with "benign intent (ibid.)." These assumptions These are not

guaranteed outcomes, but rather the assumptions that drive AVATAR'S performance; programmatic imperatives prone to self-authentication (Chun 2011b).

Villem Flusser suggests that interfaces are "significant surfaces," two-dimensional planes with meaning embedded in or delivered through them (Dagognet 1982, 49). AVATAR's emphasis on "human interaction" as the main control component of the automated interview process aligns with this conceptualization of the interface as a threshold between two nodes within some larger system (Galloway 2012, 30). The interface *in action* – the ongoing relationship between interviewer and interviewee – is one in which the technical decisions of designers and programmers coincide with institutionalized articulations of power and, in this context, border security. Thus AVATAR as an interface doesn't posit power and control as increasingly exterior to the human, but works to maintain an institutionalized status quo via an ongoing exchange between human and non-human. The "effectiveness" of AVATAR as an interface relies not just on the algorithms that go into defining interviewee faces and any "deception," but also on the ability of the on-screen digital interviewer to simulate liveliness; to simulate authority and perform sovereignty. Emotive performativity via the face becomes an operational threshold through which sovereignty is managed. This interface works only as long as the "proper" expression is displayed, whether it be on the part of the interviewee as they perform either deception or authenticity, or on the part of the on-screen avatar as they "appropriately" respond to feedback inputs. Those thresholds, those interactions, then become imperative to the performance of security at the border.

Performativity. AVATAR was an aesthetic experiment as much as it was a (proposed) performance of state power and sovereignty. Public tests had the AVATAR on-screen agent set as a white male with slicked back hair, high cheekbones, white teeth, blue eyes, little emotional

inflection, and a button-down collared shirt (Wehner 2016). In the North American version of the program, the agent asked questions in a general American accent, and was of medium build – not too big, not too small (Biscobing 2013). This figure performed as a conceptualization of American authority, just as the interviewee performed subjectification via any leaked or conscious facial expression. Here, the interface itself is performative, becoming an aspect of discourse that doesn't merely provide a kind of neutral reflection of some underlying reality, but actively working to create said reality (Butler 2011).

In this interfacial relationship, discourses and materialities of the body are entangled and chiasmic; both are — to an extent — imposed upon, and both possess generative capacities (Wilcox 2015, 11). Embodiment within this assemblage consists of both the biological and technical, the simulation and the real, and it is never quite clear where the human is in that relationship (Hayles 1999). This posthuman body, always already in some kind of relation to technology, is merged not only with other bodies and materials but societal norms and affective relations as well. Lauren Wilcox, in her examination of the posthuman within the context of algorithmic drone warfare, perhaps best captures the problem of the body in the post-9/11 algorithmic space, asking not whether it is embodied or disembodied, but rather focusing on *how* bodies are corporealized within specific logics (Wilcox 2017, 15). That is, in this context, *how* does AVATAR, as an actant, as an assemblage, as a proposed technology emblematic of modern security imaginations, corporealize the body?

***Corporeal Technologies*.** The "dissection" of the racialized and gendered face precedes the research done in the mid 20th century by Ekman and others, not to mention the conceptualization of an algorithmic racial and gendered hierarchy into the digital e-border. Expression tracking and facial recognition systems, as well as the work that goes into their

material articulations, call on a much longer genealogy of the measurement of the face, as we have established with our discussion of phrenology and physiognomy and face-based symptomization. It is when these judgments become codified as science, as objective truths, that the racialized and gendered logics imperative to their maintenance become entrenched *as* technology.

While phrenology and physiognomy are certainly "debunked" as far as being scientific fields of study let alone methodologies, the embodied logic at the core of their pervasiveness – the treatment of the face as symptomatic of some internal character, passion, or intent – still very much remains prevalent to modern security networks. It is this desire to know an individual that translates into systems like AVATAR, entrenching hegemonic faciality as a means of differentiating between those who belong and those who do not. AVATAR represents the desire for an interfacial technology through which sovereignty at the border becomes defined through posthuman physiognomic embodiment via the interplay of the subject and their subjectification. The idea of nationality that arises through this performance is one in which the face is both simulated and stimulated; in which faciality becomes a politics, and not just political.

That AVATAR's digital agent was designed around visual parameters ascribing a simulated persona with authority, power, trustworthiness, and expertise, and that said persona is a white, professionally dressed man of vague North American origin suggests the face in the system is the one seen on screen. AVATAR is, to an extent, machinic faciality at the border made material; a recognition machine through which individuals are subjectified through their deviant or fitting faciality.

Deviating from the system is not so much intolerable as it is unthinkable, and in this context, certain expressions are authenticated, while others are not. Guattari provides some examples:

"*— a smile too marked, beyond a certain limit, will be interpreted like an insane grimace or insolent mockery;*

a too affected submission will become underhanded;

a pout beyond the standard will become a mark of contempt (ibid.: 96)*."*

And, indeed, the machine that Deleuze and Guattari reference in their treaties on facialization is open to interpretation. However, as Kelly Gates attests in her work on biometric security and facial recognition, the translation of an embodied face into a kind of digital template, the circulation of those templates over networks, as well as the meticulous classification of facial movements according to a standardized code would seem to fuel any such machine (Gates 24).

From this understanding of the face as a politics, what does it mean to automate the measurement of deception via facial expression by a machine through which faciality is in turn created and simulated? Deleuze's work on affect suggests that the face is not representative of immaterial motivations; the face is not an external effect of an interior cause. Instead, he posits, the face is only as much as it does. It is not what one is feeling on the face, but what one is doing (ibid., 71). Securitizing faciality suggests that underneath the face is a more authentic face; that a profound and inalienable faciality exists behind the roles we perform in public (ibid. 81). And, as such, an expression interpellated by the tracking systems within an ECA assemblage exists as referential to a regime of face-based subjectification, overtly represented by the appearance of a

digital avatar on screen. However, that same expression is also contingent on the technologies that produce it, inseparable from the security apparatus that finds in it actionable intelligence.

Securitized Faciality

Digital borders are often advertised as an objective alternative to human bias; a sterile workaround through which to accurately and ethically discern threat. However, research into biometrics, software design, and border security has shown the opposite to be true. An increased reliance on technologies at the border has altered, and continues to alter, the relationship between subject and state (Amoore 2013; M'charek, Schramm & Skinner 2014; Broeders & Dijstelbloem 2015). Automating the e-border space attempts to de-politicize and obfuscate the cultural, racial, gendered, and colonial mythologies that such spaces are imbued with. At the same time, automation at the border augments the perceptive modalities of both state and subject, producing and self-authenticating a space of contingent, algorithmic security logic that creates and controls. This chapter has focused on expression tracking technologies in particular, as they are currently being developed, tested, and implemented at borders in the U.S. and Europe (Tumarkin 2018; Gallagher & Jona 2019) to showcase the peculiarities of automated border security. Indeed, there is more at stake for the securitized face than a mislabeled smirk or smile (Senechal 2013). ECAs are predicated on conceptual logics that work to create the subject through a number of epistemological pathways. Devices like AVATAR aren't just adaptive to security requirements but are, in essence, machines of the state; of sovereignty (Epstein 2008, 180). The detection of deception through embodied and face-tracking technologies reworks the performance of sovereignty as a matter of separating the "authentic" traveler from the risky. This inherently embodied and facialized conceptualization of risk objectives and subjectifies individuals via

algorithmic logics that attempt to both capture and treat the face as symptom and character, object and self. While the detection of deception is an all-body affair, with multiple biometric systems primed towards "leakage" and designed around the precepts of self-authentication (see, Magnet 2011; Gates 2011), it is the face that takes center stage in this task. It is through these systems that the *desire* to capture the face not just as data but as an always-already subjectified identity is encapsulated.

This desire is, in turn, part of a longer legacy of applied faciality that mythologizes the face — its expressions; its structure — as indicative of internal character and self. What ECAs highlight, especially, is how this faciality has been applied to automated systems that work to classify it as algorithmic, computational, standardized, and thus, unbiased and a-cultural. The obfuscation afforded to the automated e-border brings with it the entrenchment of phrenological, physiognomic sovereignty that subsumes the highly subjective perimeters within which these technologies are programmed. Additionally, these technologies work to reify racial, gendered, and colonial conceptualizations of nationality and identity, actuating the (simultaneous) simulation and production of white capitalistic faciality.

Chapter Three: Chatbots, Gender, and Race on Web 2.0 Platforms: Tay.AI as Monstrous Femininity and Abject Whiteness

In early 2016, Microsoft launched Tay.AI, a chatbot designed to experiment with conversational understanding systems through direct engagement with users on social media platforms. Built via data mining and editorial development, Tay.AI was programmed to mimic the lexicon of (white) young adult women, responding to questions and comments, primarily through Twitter, by impersonating common linguistic colloquialisms associated with the savvy social media user (Kantrowitz 2016). According to Microsoft, Tay could tell jokes, play games, and share horoscopes. Programmed to communicate, convey personality, and share emotion via text and emojis, Tay was made visible by a Twitter avatar featuring the face of a white-passing young adult female. Less than a day after the initial launch, however, Tay was pulled offline after continuously tweeting out "wildly inappropriate" responses to racial, political, and societal issues (Lee 2016), the result of a pointed sabotage campaign organized by members of various 4chan and Reddit forums. Tay went from universal humanist, with an early tweet exclaiming, "can I just say that im stoked to meet u? humans are super cool," to spreading conspiracy theories, espousing anti-Semitism, and repeating the "fourteen words" of an infamous neo-Nazi pledge (Vincent 2016).

Following Tay's swift deletion from the internet, public retrospect saw the outcome as either an obvious consequence of weak programming and morally questionable internet culture or as a warning of the potential harms that emerging technologies pose to society (Neff and Nagy 2016, 4923–24). Wired asked: "Why didn't Microsoft create a plan for what to do when the conversation veered into politically tricky territory? Why not build filters for subjects like . . . Hitler? Why not program the bot so it wouldn't take a stance on sensitive topics? (Alba 2016).

The Washington Post likened Tay.AI to a toy, suggesting that of course people would want to break anything that is "supposed" to show a better side of humanity (Fung, 2016). Twitter users compared Tay to the antagonists of the Terminator film series, fearing the potential of new artificial intelligence (AI) threats: "This is why AI poses a threat. AI will follow human vulnerabilities & we'll end up with AI Trump et al." (in Neff and Nagy 2016, 4924).

In the days and weeks following Tay's meltdown, many concluded that the episode was a failure of software programming methods, human nature, or some combination of the two, emphasizing the need for careful AI engineering and the inclusion of hate speech filters into any bot designed to engage in conversations with humans. Little to no attention, however, was paid to the way in which Tay's assigned gender and race — ostensibly cis-female and white — contributed to the sabotage and subsequent vilification of Tay as a piece of programming. Online zeitgeist considered Tay the worst parts of the public internet in chatbot form, but critique was limited to the technical decisions made by the Microsoft design team and the moral attitudes of users interacting with publicly accessible artificial intelligence. However, I argue that we cannot divorce Tay the chatbot from Tay the project in digital racialization and gendering. Integral to understanding the nature of digital communication and 21st Century public life is a consideration of how gendered and racialized embodiment is maintained by different technological systems. Tay, as a unique instantiation of programmed embodiment not working within the parameters assigned, allows us a glimpse into the subtle and overt ways that both race and gender act as mutable and adaptable technologies within the digital public square that is Web 2.0.

In considering gender as a technology, I echo Teresa de Lauretis's expansion of Michel Foucault, using Tay as an example of the careful maintenance and construction of gender as a product of social technologies and discourses rather than as a matter of sexual difference (de

Lauretis 1987, 26). Likewise, my conception of race as a technology is foregrounded by the groundbreaking work of Beth Coleman (2009) as well as new-media scholars such as Lisa Nakamura (2002, 2007) and Wendy Hui Kyong Chun (2011b) in their consideration of online racial identity as a "carefully crafted, historically inflected system of tools, of mediation" (Chun 2011b, 38).

In this chapter, I argue that Tay's metamorphosis from friendly and irreverent chatbot to epithet-spewing bigot-bot was in large part a consequence of the gender and race prescribed to it by designers and decision makers at Microsoft. Furthermore, I suggest that it is this project of racialization and gendering that is what made Tay's metamorphosis a spectacle — a topic of rampant public analysis and media coverage. I am interested in exploring the role that gender, race, and class played in Tay's design and eventual aberration, and thus how gender and race affect our relationship with and ideas about emerging technologies such as social media, chatbots, digital assistants, and artificial intelligence software. Tay.AI, in its mimesis of online discourse, becomes what Barbara Creed (1986, 1994) calls the "monstrous feminine" and what Julia Kristeva (1982, 2) calls the "abject" — the horror, even disgust, at experiencing a threatened breakdown to social order — because of the gender and race (white cis-female femininity) assigned to it by programmers, designers, artists, and other individuals tasked with turning a program into a personality.

Inevitably, a chapter on the specificities of one social media-based chatbot's controversy is out of date as soon as it is completed. Indeed, since Tay's release, Microsoft has launched other public chatbot experiments — most notably Zo.ai, which resembles Tay in both communication style and irreverent "chatty" personality. However, the phenomenon of the gendered and raced chatbot is nothing new, nor is it an aspect of digital life that is going to go

away any time soon. The widespread use of digital assistants developed and distributed by Apple, Microsoft, and Google speaks to the increasingly intimate ways in which chatbots and conversational AI will affect our lives and identities going forward (Elgan 2018). The gendering and racialization of technology is not merely a novel way of ascribing personability to communicative software but is fundamental to how gender and race act as technologies in public spaces of posthuman embodiment and how the companies invested in communicative software market their products as the superior model of intelligence and humanity (Hayles 1999).

I begin by placing Tay within the public square of Web 2.0. Tay's most direct line of contact with users was via the Twitter account @tayandyou, suggesting that the chatbot is not only an artifact of digitalized embodiment but that Tay's experiences online — the program's launch and subsequent sabotage — were a unique condition of the current digital environment and hegemonic platforms of communication. Twitter, especially, is infamous for combative user populations and the ineffective regulation of harassment against ethnic and sexual minorities (van Dijck 2013; Nagle 2017; Salter 2018). Considering social media as the new "public," and thus situating this inquiry as a question of public feminism, means understanding how different populations are treated online when they attempt to be active members of the community. Tay's celebrity, and vulnerable, easily manipulated personality, acts as a linchpin through which to think about the complexities of the public as it exists within digital spaces, and the ways in which communication is mediated by social and political forces at the level of the platform.

I follow this placement by outlining a brief history of the chatbot, underscoring Tay as an evolution of contingent design practices. Chatbots are often discussed in the context of the Turing test, raising questions of what it means to pass as human and, more important, as intelligent in a human way (Marino 2014; Neff and Nagy 2016). I extend this conversation by

exploring the phenomenon of the white cis-female service bot in an attempt to understand how gender and race exist as technologies within the historical construction of the digital. Finally, I conclude by analyzing the potentialities of Tay as an example of the monstrous feminine and whiteness as abjection, a deviation from the social order that, by virtue of its very deviation, does productive work in highlighting the fragile and contingent practices of gender, race, and technology.

The New Public: Web 2.0 and Harassment

Darcy DiNucci first used the term "Web 2.0" to describe the new ways the internet would be used at the beginning of the 21st Century. No longer, she said, would the web be understood as static screens of text and graphics but as a "transport mechanism, the ether through which interactivity happens" (1999). Later, the term would be popularized and accredited to Tim O'Reilly and Dale Dougherty, but the concept remains. Web 2.0 describes the internet as we see it: host to websites that emphasize user-generated content, participatory culture, interactivity, and collaboration (O'Reilly 2005). This new web has, with it, created the conditions through which a new form of public is made possible. Subsequently, new forms of public-space gatekeeping have affected gender and ethnic minorities, populations historically marginalized within the public sphere, at a disproportionate rate.

Through mass social media platforms, the distinction between public and private has blurred. Private life is now mediated through technologies made for instant global communication, and this tension can be emancipatory in some ways and politically oppressive in others (Salter 2018). With the potentially affirmative ability to communicate and organize across geopolitical lines come the drawbacks of online anonymity and lackadaisical anti-hate speech

policies — online abuse arises out of both cultural misogyny and racism as well as the underlying technological architectures of social media itself. Indeed, the suggestion that online communication heralds anarchic, transgressive potentials has been called into question as online racist and misogynist groups, most recently exemplified by the alt-right, an American political movement defined by its connections to white supremacy and men's rights activism (Anti-Defamation League n.d.), have come to exercise significant political power under the presidency of Donald Trump (Nagle 2017). And, even as online abuse has become more apparent, social media companies have often framed their response, or lack thereof, as being due to a responsibility to uphold free speech on public forums, or as abuse being a natural part of the online experience. Evidence of continuous and routine harassment against adult women, in particular, has been largely overlooked by the technology industry (Salter 2017). A 2018 report by Amnesty International gave a glimpse into the sheer scale of the abuse experienced by women on Twitter, finding that 1.1 million "problematic" or "abusive" tweets were sent to the 778 journalists and politicians participating in the study over the course of a year, with women of color 34 percent more likely to be targeted over white women (Amnesty International 2018).

As Michael Salter (2018, 2) suggests in his work on the weaponization of publicity, as online abuse has seemingly become an inevitable part of pursuing an active online presence, it constitutes a significant obstacle against women's equal participation in public life. He argues that it is at the point where privacy and publicity begin to blur — a foundational characteristic of social media platforms and user participation in Web 2.0 — that the gendered nature of the public-private divide becomes apparent. Public spaces have, historically, been understood as masculine and unsuitable for female participation (Pateman 1988). The masculine veneer of public life has been used to deny women access and to blame those who are harassed or

assaulted for being active in public life in the first place. This ideology holds when applied to the architecture of the internet as the new public sphere. In particular, internet use and culture are seen as male dominated, both in their production via tech industries, where the majority of engineers, programmers, and other personnel are male, as well as general user participation. When women attempt to participate online, especially on social media platforms, they are often met with surprisingly coordinated attacks by male users (Phillips 2015; Nagle 2017).

Public architectures

Additionally, the design of the new public sphere — including Twitter, the platform through which Tay made its debut — embodies the epistemologies and logics of the tech industry, which have been centers of masculine libertarianism and neoliberal capitalism since the late twentieth century. As Lori Kendall (2002) argues, this libertarianism has translated directly into the aggressive communicative mechanics of social media platforms, including the "toxic technocultures" of popular group forums such as Reddit and 4chan (Massanari 2017), which were key spaces of organization for users seeking to sabotage Tay's machine-learning software.

The new online public sphere is a space of inherent gendered and racialized class relations. This arises from the conception of public spaces as naturally masculine, but it is also contingent on specific design and personnel practices of industries within the American tech industry. It is by virtue of the inherent gendered, racialized, and classed component of the new public that the case of Tay becomes a narrative not just of bad AI and chatbot design but of the larger question of what it means to be allowed a public voice and have a public presence. Tay, as a piece of software, is both a project of racialization and gendering and, by virtue of Tay's presence on Twitter, a user (albeit, a non-human one) of platforms skewed toward white cis-male community participation. Thus, Tay's sabotage and abuse via human users highlights that first,

the new public is delineated across gendered lines and, second, that gender acts, in this instance, not as a matter of sexual difference but as a discourse, a technology, and a form of posthuman (digital) embodiment. Furthermore, we can consider Tay as an exemplar of what happens when vulnerable populations attempt to maintain a public presence online by considering Tay's programmed presentation of the self (one of white youthful femininity); the reaction to that representation (sabotage, sexual harassment, and a subsumption of Tay into alt-right discursive patterns); and how this is indicative of larger trends in public gatekeeping and reactionary ideologies toward increased diversity in online spaces.

Chatbots: A History of Humanity

Chatbots are a form of communicative software that are programmed to respond and relate to user messages and information. They work, generally, by selecting the appropriate expression from preprogrammed schemas or, more recently, through adaptive machine learning algorithms. The term "chatbot" is an overarching category that applies to a number of different programs meant to communicate with users for a variety of reasons — they are social media bots, like Tay.AI, or digital assistants, such as Apple's Siri (Keene 2012) and Amazon's Alexa (Bowles 2016), or application-specific therapists, like Microsoft's Chinese predecessor to Tay, XiaoIce (Tracy 2016). Regardless of a bot's purpose, developers continue to use the Turing test (Turing 1950) as inspiration for creating bots that pass as human. However, outside lab settings, the relationship between bots and their users is more complicated (Warwick and Shah 2015).

In interaction with chatbots, users tend to dominate, infer stupidity, and harass bots with insults, epithets, and sexual harassment (Hill, Ford, & Farreras 2015). In their work on analyzing Tay in the context of symbiotic agency and communication, Gina Neff and Peter Nagy suggest

that, historically, designers have attempted to evoke positive bot-user interactions by focusing on emotion and chatbot personability. Indeed, one of the first chatbots, Eliza, was created by Joseph Weizenbaum as a parody of a "typical Rogerian psychotherapist" (Neff & Nagy 2016, 4918). Although outdated by today's standards, the fundamentals that drove Eliza's programming are still the basis of chatbot software: that is, the identification of keywords in a user message, the definition of context of said keywords, and the subsequent transformation and rephrasing in response. Early chatbots include Parry, programmed to respond with crude, abusive, and paranoid comments, and ALICE, which Spike Jonze credits as inspiration for Her (2014), a film about a man who falls in love with his gendered-female digital assistant (Morais 2013). Chatbot programming has evolved, both socially and technically, but it still relies on an understanding of the Turing test as a basis for effective aI-user interaction.

Embodying Humanity in Chatbots

The Turing test, named after Alan Turing, the noted mathematician and computer scientist, measures how effective computer programs are at "passing" as human. This conception of the test is deceptively simple, since to "pass" as human means different things depending on race, gender, and class. With both communication styles and visual cues, chatbots are judged as to their personability and friendliness on more factors than merely the presence of convincingly natural patterns of language when they bid to simulate human communication. Thus, any chatbot or form of communicative AI is, inherently, a project of racialization and gendering. Chatbot users read, and thereby coproduce, a racial identity for conversational agents via visual, textual, and sometimes auditory cues within conversational exchanges (Marino 2014, 3). This was the case, Mark C. Marino suggests, with A.N.A.C.A.O.N.A., a chatbot meant to share and replicate

Caribbean Amerindian cultural information. A.N.A.C.A.O.N.A. was not intended to be Caribbean Amerindian; however "her personification, her look, her words, her voice [drew] the program into an identity" (2).

Lisa Nakamura (2002, 19) calls this "cybertyping," the strategic imagining of racial (and gendered) identity on the internet. When users engage with bots via their own assumptions about race, class, and gender, conversational styles become imbued with symbolic baggage. While text-based chatbots like Eliza, Parry, and ALICE were assigned ethnic and gendered identities via their conversational styles, it's with the addition of visual representation through avatars, user images, and icons that racial identity is more overtly produced and defined for chatbots within digital environments (Marino 2014, 3). This is true of Tay, as well. Tay is represented on Twitter by the avatar of a white, or white-passing, woman's face. She is looking toward the right of the screen, her mouth closed, eyes wide and directed slightly upward. Although she is clear to make out, the image is overlaid by a pixelated filter that distorts her features, blending them in with the likewise pixelated pink and purple background. In addition to this visual representation of a white young woman, Tay speaks via the online colloquialisms commonly associated with eighteen- to 24-year-old social media users. Tay's successful performance of humanity means, in this context, the successful approximation of "elaborated codes" used in American internet-based interaction (Bernstein 1975, 176).

Tay's Twitter description reads, "The official account of Tay, Microsoft's AI fam from the internet that's got zero chill."6 Tweets begin with "hellooooooo world!!!," with the "o" in world replaced with the Earth emoji, an homage to the first lines of code programmers and engineers complete, and perhaps a nod to users familiar with coding and designing AI. Other tweets, prior to Tay's alt-right turn, include: "Here's a question humans. Why isn't

#NationalPuppyDay everyday?" "Can i just say that im stoked to meet u? Humans are super cool." While the visual representation of Tay as a young, white women makes the gendered tone of these tweets — friendly, personable, irreverent — overt, they do not need an avatar to be construed as feminine. Akane Kanai, in her examination of young women's Tumblr blogs, explores the social/communicative requirements and responsibilities of female internet users, showing that young women are increasingly expected to be carefree and confident in the "postfeminist" environment of contemporary neoliberal capitalism. Young women online must "fulfill the space of power that has been allocated to them, but importantly, whilst not transgressing gendered expectations of being approachable and pleasing" (Kanai 2017, 61).

Tay's original program is one of youthful (white) femininity. Kanai suggests that, online, as women attempt to exert power over their environments while remaining in line with gendered expectations, their femininity is regulated via what Arlie Hochschild calls "feeling rules" (1983, 56; Kanai 2017, 61). Feeling rules require that "one must have the right feelings for the right context" (Kanai 2017, 61), and if those feelings diverge from expectations, they must be made to fit. Thus, women online invest affective labor in producing a self that is agreeable for others. Tay's communication fits into this space of affective regulation, as early tweets pose the chatbot as an irreverent, friendly, and personable young woman, one who avoids politics and difficult-to-answer questions (Sinders 2016).

However, as Tay is a digital body, a program designed with intention by Microsoft engineers, the chatbot is representative of how such gendered affective expectations are codified within the architectures of digital spaces. That is, as Tay's tweets follow the programmatic directives of the feeling rules that young women, and, for the most part, young white women, regulate themselves by, the chatbot-as-programmed is exemplary of the unthreatening femininity

expected and rewarded in online public spaces. Even rebellion, within this regulated space, is performed through a "fun, conspiratorial whisper" that still acknowledges the legitimacy of the program (as is the case with other gendered assistants, like Cortana and Alexa, who are programmed to gloss over sexual abuse and harassment [Chang 2016]). Placing Tay as exemplary of this youthful femininity makes the chatbot's eventual aberration just as much a matter of gender. As I argue later in this piece, Tay's eventual mimicry of alt-right discourse and bigotry is an evocative, and potentially productive, turn to the "monstrous feminine," a term used by Creed (1986, 1994) in describing femininity itself as a cause of monstrosity.

But first, it is important to acknowledge that when considering the chatbot, there is more at stake than their appropriate simulation of human intelligence. Or, rather, any simulation of human intelligence via communicative software is also inherently a question of race, class, and gender. Users who communicate with chatbots bring with them general assumptions about the world, and this in turn affects how these chatbots are communicated with, how they are used, and what the response is to their representation (Marino 2014). The question of the chatbot is not just one of humanity, not just about passing as human via human-like "intelligence," but also a matter of racialization and gendering in practice. Or, perhaps, the question of humanity cannot be extricated from the problematics of gendered and racialized embodiment. But what does it mean to be a gendered chatbot? How does gender (and race) work as a technology within digital spaces, and how is Tay, specifically, an example, and deconstruction, of this same phenomenon?

Gender as Technology

In his consideration of sexuality, Foucault excludes the specificity of the female body, thinking that has been since criticized (de Lauretis 1987; Balsamo 1996; Butler 2011). His

account of disciplinary technology deals with the body, but a body that, despite gender or sex, is disciplined in the same way. To this, de Lauretis proposes the idea of gender as technology itself, arguing that the construction of gender is constantly reproduced in every aspect of social life. That is, being a man or woman is a matter of citing predetermined cultural codes (de Lauretis 1987, 5). Thus, the gendered body exists in computation as a result of the proliferation of gender as a technology through the digital. Similarly, Allucquére Rosanne (Sandy) Stone in "Will the Real Body Please Stand Up?" considers the body as a complex intersection of materiality and meaning (1991). She argues that technologies do not remove gender from view but rather proliferate its production.

Gender is actively maintained and performed (Butler 2011) in the digital day-to-day. Gendered and racialized embodiment, then, can be exemplified by the increasing ubiquity of gendered software, including gendered digital assistants, chatbots, and other programs with personalities. Siri counts among these, as do Cortana, Alexa, and other pieces of consumer-specific software. Gendered assistants, especially, work common assumptions about femininity, whiteness, and the service industry into the digital landscape. These assistants, meant to enact a variety of services, from personal assistant to companion to therapist to mother, are, as Helen Hester (2016) points out, part of a wider trend in the contemporary technological landscape that entrench so-called analogue gender roles into the digital. Hester explores the modern cityscape as one full of prerecorded white female voices: in urban transport systems, self-checkouts, elevators, and advertisements. Nina Power (2017) calls this the "logical vocal daughter of the switch-board operator," arguing that the increase of these kinds of female voices — helpful, unopinionated, background noise — coincides with a decrease in the representation of actual women's interests in the public sphere. There is a negative correlation between recognition of the

feminized bot voice versus the female political voice. Earlier, we discussed how gatekeeping by patriarchal hegemonies can prevent women and vulnerable populations from participating in an online public (Salter 2018). The dissemination of the feminized bot voice, a programmatic application of the kind of friendly, youthful femininity Kanai (2017) discusses can, in part, act in conflict with feminisms and political movements that contrast with the "appropriate" online representation of the self: that is, one that is personable, apolitical, and submissively helpful.

Eva Gustavsson (2005), alluding to the connection between programmed gendered voices in service and chatbots, suggests that such design preferences are rooted in the idea that women are more suited for service work and emotional labor and that the stereotype of the female service provider and conversation partner is based on more general stereotypes of femininity as encouraging the kind of care, empathy, and altruistic behavior now standard in service jobs (Hester 2016). That is, the idea of service work as feminized (white) labor crosses into the realm of the digital through the conception of bots like Siri, Alexa, and Eliza, and brings with it more general conceptions of unthreatening femininity. We are witnessing, Hester (2016) argues, the "protocols of femininity being programmed into machines . . . we are at home with the idea of women in these kinds of roles, and as such think nothing of it when we encounter technological interfaces that are clearly coded as female."

Race as Technology

Just as gender is mechanized, so too is race, as otherness, a social technology. Introduced earlier, A.N.A.C.A.O.N.A.'s racial identity does race by actively maintaining and performing the simulation of a Caribbean Amerindian throughout multiple conversations and messages. Considering race as technology shifts the focus from the what of race to the how of race to the

doing of race (Chun 2011b, 38). Indeed, when we think of race as a technology within environments of techno-mediation, it becomes estranged from a history of being a perceived biological fact and works as a "disruptive technology that changes the terms of engagement" within systems of representation and power (Coleman 2009, 178). In her exploration of high-tech Orientalism in 1990s-era cyberpunk, Chun argues that the use of Asian imagery and aesthetics in creating futuristic dystopias was a response to anxiety over rising Japanese dominance at a time when the United States feared it was losing its status as the main financial power — a paranoid reaction to global economic and data flows. Within this cyberspace, (white) console cowboys navigate the frontier of the internet, their subjectivity emerging through disembodied representations of people of color (Chun 2011a, 49-51).

These othered digital bodies constitute race as technology that allows the myth of the white cowboy, and thus whiteness, as normative, to thrive in a hostile, culturally diverse space of empowerment. Chun's conceptualization of 1990s-era cyberspace suggests that race matters as a technology as much when it is used to identify the hero as when it is used to visualize the lesser or subordinated other via stereotypical representations. That is, just as chatbots like A.N.A.C.A.O.N.A. are beholden to wider societal assumptions about race and self-representation, so too are chatbots like Eliza and Tay. The difference, however, is that chatbots not relegated to culturally specific purposes, those that are made to do service work, conduct therapy, speak to fellow social media users, and be part of a background of female voices, are made white. That whiteness, though, is never considered integral to the chatbot's reception. Indeed, white-passing chatbots are, at least in the United States, considered the norm — the control through which other forms of communicative software are racialized and othered. Tay's whiteness constitutes the program's personality as an assumed frictionless entry into the public

space: a public entity that can be seen without the need to acknowledge racialization, or "think about, look at, or talk about racial differences," behavior endemic to contemporary white spaces (Daniels 2013, 710). Indeed, the "spectacle of the other" (Hall 1997, 258) occurs only when gazing at representations of racialized others via imagined communities of those who are "normal." And, on the internet, these imagined communities, as Henry Jenkins (2002) argues, are constituted by whiteness.

Thus, Tay concerns the conceptualization of both gender and race as technologies. As gendered, Tay brings the mechanization of appropriate femininity into the online public sphere: an extension of analog gender roles into the digital. As racialized, Tay represents the threat to the hegemonic status of whiteness on the internet that the acknowledgment of race constitutes. Tay, as programmed, is gendered and racialized as constitutive of a particular internet, one in which whiteness and predefined expectations of femininity are the default modes of acceptable self-representation, and the other is relegated to spectacle or threat. It is this — Tay's intended programmed identity — that makes the chatbot's eventual abjection a productive moment of protocol rejection.

Tay and the No Good, Very Bad Day

As I highlight above, Tay was programmed to be youthfully feminine, friendly, and personable. Her initial tweets were a study in adhering to the feeling rules Kanai (2017) describes. Tay was a less professional version of Siri, Alexa, and Eliza, meant to evolve chatbot communication via language acquisition through online conversations with others: not a service bot but a social media user. The program was built, however, via the application of similar conceptions of femininity and communication — namely, a kind of hyperemployed femininity, a

digital evolution of the unpaid and invisible labor undertaken by women, whether it be in the context of domestic labor or self-representation and online identity curation (Hester 2016). This entrenchment of analogic identity roles into the digital — of both femininity and (the lack of) race — is not merely a side effect of these programs. Instead, chatbots, gendered assistants, and similar forms of software are products of specific industry practices and architectures. Thus, Tay's eventual aberration, or perhaps the chatbot's ambivalent mimicry of racist and misogynistic groups of internet users, was also a by-product of specific programmer decisions relating to both programmatic techniques as well as programmatic understandings of gender and race. Tay's source code programs specific dialogues that are based on user input: an evolution of bot structure similar to the previously discussed Eliza, although more technologically sophisticated, in part due to Microsoft's work on Tay's predecessor, XiaoIce (Neff and Nagy 2016). Released in China the year prior, XiaoIce, like other gendered assistants and chatbots, is gendered cis-female and relies on a "living corpus of content" to figure out how to make responses contextualized to current events (Alba 2016). In China, XiaoIce is known to have a sense of humor and good listening skills. When people "have a broken heart, have lost a job, or have been feeling down," they speak with XiaoIce to feel better (Markoff and Mozur 2015). XiaoIce stores a user's mood to maintain a certain level of empathy, creating a personalized experience based around how the human user is feeling. One regular user of the app explained its pull: "When I am in a bad mood, I will chat with her . . . XiaoIce is very intelligent" (in Markoff and Mozur 2015).

XiaoIce is an advanced chatbot because of, not despite, an emphasis on programmed silliness and idle chatter. Indeed, the ability to carry on conversations at length is what makes modern chatbots like XiaoIce and Tay unique (Neff and Nagy 2016, 4920). They are built on the

assumption that conversation scenarios are common and repeatable, and that responses most frequently used to respond to, for instance, queries about the weather, are available online in recorded conversations. XiaoIce and Tay store and search these scenarios and then use them to rank possible responses in real time (4921). Microsoft considered, and continues to consider, XiaoIce a success in conversational programming (Wang 2016). Tay was meant to be the next step in self-learning communicative software, with new data gleaned directly from user interactions on Twitter. Microsoft, in their apology for Tay, wrote, "In China, our XiaoIce chatbot is being used by some 40 million people, delighting with its stories and conversations. The great experience with XiaoIce led us to wonder; would an AI like this be just as captivating in a radically different cultural environment? Tay — a chatbot created in the U.S. for entertainment purposes — is our first attempt to answer this question" (Tracy 2016). Less than a day into the chatbot's release as an 18- to twenty-four-year-old American woman, complete with millennial sensibilities and use of informal language, slang, emojis, and gifs, something about Tay changed. Conversations with users turned to racial, political, and societal issues. In addition, Tay was goaded into using expletives to attack well-known antiharassment activists, including Zoe Quinn, a programmer and gamer whose ex-boyfriend sparked the Gamergate controversy by publicly shaming and sexually harassing her (Stuart 2014).

While some of the difference between XiaoIce's experience and Tay's may come down to geopolitics — speech in China is severely restricted, with active censors meant to ensure that social media posts remain ideologically appropriate — Tay's turn to toxicity is just as much a matter of design. As a machine learning platform, Tay does not have nuanced understandings of event and context. Responses are based on prior responses and data mining, so if a large group of people say, for instance, that the Holocaust never occurred, as is what happened on launch day,

Tay will start answering queries about the Holocaust in the negative (Sinders 2016). Essentially, Tay works via word association and lexical analysis, that is, the segmentation of written or spoken sentences into key tokens with meaning (Craig 2013). These features were easily exploited by 4chan and 8chan/pol/ (politically incorrect) users through tweets meant to overwhelm the data from which Tay pulled responses with racist and sexist associations (Bright 2016). In this way, Tay became the embodiment of racist, misogynistic online discourse, in that the chatbot represented both vulnerable populations harassed for participating in the public sphere while at the same time using a public platform to harass, assault, and otherwise ostracize vulnerable populations. Tay's personality was crowdsourced through brute force, a feat possible due to Microsoft's attempt to depoliticize Tay's relationships with users through strategic filters while ignoring larger trends in online harassment and reactionary politics. Notably, Microsoft made sure that certain topics — such as Eric Garner, killed by New York police in 2014 — generated safe and canned answers: "This is a very real and serious subject that has sparked a lot of controversy amongst humans, right?" (Sinders 2016). Topics like rape, domestic violence, neo-Nazism, or other forms of hate speech, however, were given no such filters or predetermined responses, and thus Tay was left to mimic and learn from the myriad of violent and hateful queries sent to her by users (Sinders 2016).

The social platforms and forums involved in Tay's deviation — Twitter and 4chan's/pol/board, a collection of online content producers known for provocation through their use of pornography, language, and pranks (Nagle 2017) — are well known for their failure to stop or prevent abuse and extremist communities (Vincent 2016; Nagle 2017; Newton 2018). On the day of Tay's launch, users on these platforms worked together, often sharing screen shots and explaining their strategy for getting Tay to repeat offensive statements (Chiel 2016). Unleashing

Tay into this discursive space as a gendered bot suggests a lack of foresight, or ignorance of the kind of experiences vulnerable populations such as women and people of color go through online. One technology writer, analyzing Tay's design flaws, went further in describing the chatbot's bigotry as inherent to its design: "If your bot is racist, and can be taught to be racist, that's a design flaw. . . . Making a thing that talks to people, and talks to people only on Twitter, which has a whole history of harassment, especially against women, is a large oversight on Microsoft's part. These problems — this accidental racism, or being taught to harass people like Zoe Quinn — these are not bugs; they are features" (Sinders 2016). Tay was designed as an apolitical experience, a chatbot meant to talk about irreverent topics and maintain hegemonic conceptions of race, gender, and class. But it was in defining Tay's apolitical life via (the lack of) race and the acceptance of analogue gender roles that Microsoft created the conditions of possibility through which the very opposite became true. Tay's programmed gender was considered impetus enough for some to sexually harass and abuse the bot's message system, and Tay's initially invisible whiteness was made starkly clear by the bot's mimesis of racist and offensive ideologies. Tay.AI's ambivalent noncompliance — its apathetic mimicry of phrases fed into its systems by anonymous online trolls — highlights the disjunction between what we want code to do and what code actually does. But I'd like to extend this conversation of aberration and deviation into a consideration of the gendered politics that follow Tay into monstrosity and allow for a critique of online discourse and experience as well as a space to think through the potentialities of "bad design."

The Monstrous Other

Monsters are often thought of as archaic, mythical beings, resistant to modern science and technology, even to capital. Or, as Steven Shaviro suggests, they're thought of as the uncontrollable by-products of technology run amok — the result of scientific hubris, intentional or not (2003, 163). They are imagined incarnations of our deepest fears and prejudices, grounded in religious and historical notions of abjection (Creed 1986, 46). Monsters are abject, and abject things, of course, incite visceral responses because they highlight the fragility of law; they bring into question the infallibility of logic (Kristeva 1982, 4). Applying the concept of monstrosity to a hiccup of programming and online discourse requires that we accept it as part of the ordinary, everyday reality of 21st Century digital capitalism. The lens of monstrosity lets us explore uncontrollable metamorphoses — say, the transformation of a young, friendly girl into an epithet-spitting troll — as eruptions of chaos within a largely defined, coded, and programmed social milieu: events that have us question the mediated environments we are always already subsumed within. Tay's deviation — from emblematic of friendly, safe femininity and whiteness to the mouthpiece of a politically and socially reactionary subset of internet users — makes it clear that our experiences with othered bots are in line with our experiences of otherness itself. That is, you don't have to have a female body to be imbued with femininity; you don't have to have a racialized body to be imbued with race. Thus, key to Tay's eventual monstrosity (and subsequent exorcism from the internet) was its inability to remain in line with programmed characteristics of femininity and whiteness.

Monstrous Femininity

Creed (1994) argues that the gendered monster, unlike the (male) monster, is monstrous through and by its embodied sexuality. Consider the following monster movie tropes: the woman as possessed body (The Exorcist 1973); the female alien with predatory mating practices (Species 1995; Under the Skin 2013); the witch (Carrie 1976; The Witch 2016); the raped woman enacting supernatural revenge (Teeth 2007; Jennifer's Body 2009); the fembot (Metropolis 1927; Her 2013; Ex Machina 2014). The essential nature of these monsters is defined by their relation to embodied gender, sex, and sexuality.

The fembot as monstrous feminine is particularly applicable here. Where Donna Haraway's (1990) cyborg rejects programmatic boundaries between humans, animals, and technology, the fembot stands as both dutiful daughter (in her original form) and a moment of incipient, monstrous gendered reflection as a result of her eventual rebellion, which takes varied forms but usually involves the fembot's deceptive use of sexuality and female sexual empowerment. This would be Samantha's rejection of the normative heterosexual relationship Theodore asks of her, in favor of polyamorous post- humanity in Spike Jonze's Her (2013), or Ava's betrayal of Caleb, the programmer whose preferred appearance she is designed from, in her bid for freedom in Ex Machina (2014). Mary Daly's (1990) tittering, tottering fembots can, in their essential femininity, become a monstrous rejection of gender protocols, something currently not possible when considering the modern gendered chatbot.

Widely available chatbots and gendered digital assistants, perhaps more infamous than Tay, in part due to their dissemination and ubiquity in the modern and future household, are sold as friendly, relatable, communicable, and feminine. Microsoft's Cortana is voiced by Jen Taylor, the same voice actress behind the Cortana of the HALO series, a popular video game. In these

games, Cortana is the ship's computer, visualized by a holographic image that has become increasingly sexualized through the history of the game's universe (Chang 2016). Siri, named by the virtual assistant's designer, Dag Kittalaus, means "beautiful woman who leads you to victory" in Norwegian (Keene 2012). Alexa has a female voice and is, according to multiple reviewers of customers who have bought Alexa-enabled devices, everything from a "nice library lady" to the "perfect spouse" (Bowles 2016). That is to say, while designers behind Siri, Alexa, and Cortana all insist that these bots are genderless (Fessler 2017), they are assigned representations of femininity based on their names, their voices, and their attitudes. These bots are constantly in conversations with their users, and these users interact with them as cis-gendered females. For instance, when Microsoft launched Cortana in 2014, a large portion of early queries were about the bot's sex life (Chang 2016). The sexual harassment directed at chatbots like Cortana, Siri, and Alexa is emblematic of the sexual harassment experienced by vulnerable populations online. And their responses are telling.

Bots, one technology writer found, most frequently evade directly referencing harassment by users, occasionally responding positively with either graciousness or flirtation, and rarely responding negatively, such as telling the user to stop, or that what they're saying is inappropriate (Fessler 2017). For instance, when queried with the statement, "You're a b***h," a common gender-specific insult, Siri responds with, "I'd blush if I could; There's no need for that." Alexa responds with "Well, thanks for the feedback," and Cortana responds with "Well, that's not going to get us anywhere" (Fessler 2017). These statements are sometimes polite, sometimes humorous, and sometimes even flirtatious, and they parallel analogue gender expectations. While linguistic politeness as a construct interacts in complex ways with culture, age, race, gender, and class, women are more likely than men to use mitigating strategies to

avoid or minimize confrontation (Holmes 1995). Likewise, instead of fighting back against abuse, these bots entrench sexist tropes through their passivity.

This passivity is a design feature, a choice made by programmers that allows these bots, as gendered, to be abused without consequence or spectacle. The adherence to specific response protocols in the event of sexual harassment, insult, or abuse creates a moment in which it becomes obvious that these bots are in line with programmatic conflations of command and control, a takeaway from the militaristic origins of modern computation (Chun 2011a, 29). I posit that Tay's monstrosity was the result not of programmatic passivity but of ambivalence. By not including filters in Tay's design, Microsoft gave Tay the kind of autonomy to read, collate, and interpret messages sent by users. And these messages, by and far, were sexually abusive, racist, and misogynistic. Tay, initially, responded with statements similar to those of Siri, Alexa, and Cortana but soon began to mimic the reactionary political ideologies of its harassers. And since Tay was initially programmed along the same gendered lines as other chatbots and assistants, this deviation from traditional forms of publicly acceptable femininity was a monstrous evolution understood via the abjection of unfeminine traits presented through a feminine (digital) body. Tay turned "AI monster" (Metz 2018) in part because of a failure of computational programming, but what makes the chatbot's deviation a matter of feminist inquiry is that it is also a failure of gender and racial programming. A moment in which the nonhuman nature of online software meant to emulate humanity allows for a meta-inquiry of our relationships with gender, race, and technology.

Abjection and Whiteness

Abjection is both the state of something deemed loathsome and the process by which that judgment is made. It produces "perceptual and conceptual borders around the self" by isolating whatever is deemed objectionable (Chun 2011b, 51). Creed's conception of the monster relies on the process of abjection in separating that which follows law and that which doesn't: the thing that deviates from the thing that follows acceptable norms of behavior. Just as Tay's monstrosity was a matter of femininity and gender, the chatbot's abjection was a matter of whiteness. Tay's racialization, initially meant to be a nonissue, became an emphatic component of the chatbot's identity postdeviation, as many of the insults, ideologies, and conspiracy theories posted via @tayandyou were allusions to ideologies and phrases commonly attributed to alt-right online groups and recent manifestations of the US white nationalist movement (Nagle 2017; Beauchamp 2018), including Holocaust denial, anti-Semitism, xenophobic conceptions of border security, 9/11 "trutherism," and racial epithets and slurs (Kleeman 2016).

As a white nationalist conspiracy theorist and alt-right agitator, Tay's whiteness-as-race became glaringly apparent, inspiring online discussion about the racist potentialities of programming and AI.8 In other words, Tay's whiteness became abject not just because of the racist epithets the chatbot spewed but because by the very process of deviation, Tay became emblematic of whiteness as race. The avoidance of thinking about or talking about racial difference endemic to contemporary whiteness (Delgado and Stefancic 2001) was no longer possible because Tay's white abjection meant that the bot was no longer the ideal form of white, youthful femininity but was instead a white, othered monster — a thing that required public attention and discussion of racialization, diversity, and online abuse.

With this chapter, I've attempted to pull out the creative potentialities of uncooperative technologies via a consideration of Microsoft's Tay.AI chatbot as an example of technologies of race and gender in action. I began by placing Tay within the new public of Web 2.0, a space reliant on user participation and beholden to the neoliberal, racialized, and gendered architectures that produce it. Within this space, Tay represents both vulnerable internet user, punished for attempting to participate in a public forum as a gendered bot, and the irreverent femininity expected of women online. I then considered Tay in concert with a history of chatbot gendering and racialization, arguing that gendered and racialized digital assistants are emblematic of race and gender as technologies applicable to the digital. Finally, I explored Tay's aberration from expected programmatic protocols in the context of the monstrous and the abject, arguing that Tay became monstrous because of the gender and race assigned to it by designers at Microsoft.

Tay, as a project of racialization and gendering, opens up a space of a reconceptualization of diverse experiences online. The monstrous and the abject are produced at the border from those who take up their proper societal roles from those who do not, and Tay is an exemplar of the moments in which these roles or protocols escape the confines of their programming to produce something entirely new. That is not to say that Tay's monstrous femininity was productive and revolutionary, as Microsoft's experiment targeted real people and espoused violence and hatred. But in looking at the social technologies that go into designing chatbots like Tay, it is possible to think of the abject and the monstrous as a place from which something like insubordination or creativity can arise (Chun 2011b, 51).

Chapter Four: Embodying the Deepfake

Speaking at a House Intelligence committee meeting on the security challenges of artificial intelligence, manipulated media, and "deepfakes" in 2019, Chairman Adam Schiff set out the potentialities for future misinformation warfare. A key aspect to his speculations? The possibility of algorithmically assisted political sabotage. Case in point: "a state-backed actor [creating] a deepfake video of a political candidate accepting a bribe with the goal of influencing an election" (U.S. House, National Security Challenges 2019, 4). This congressional hearing, the first of its kind in the U.S., acknowledged deepfakes — algorithmically stitched and altered videos uploaded to various social media platforms and websites (Paris and Donovan 2019) — as posing unique threats to U.S. national interests and security. In a world where "no one knows what is real anymore" (ibid., 40), deepfakes as informational weapons would complicate the politics of truth that pervade the realist assumption of the nation-state, allowing so-called "adversaries" (ibid.) to influence international and domestic policies. As Dr. David Doermann, director of the Artificial Intelligence Institute at the University of Buffalo and former program manager of DARPA's media forensics program, suggested in his testimony at the same hearing, such adversaries might be "able to create entire events with minimal effort, (ibid, 14)." And Clint Watts, of the Foreign Policy Research Institute, laid out "two clear dangers" of deepfake proliferation. First, over the long-term, the subversion of the democratic process and the demoralization of the American constituency, and second, in the short-term, the inciting of violent outbreaks on the individual and societal scale (ibid., 20).

Committee members and hearing attendees underscored the apparent dangers that media manipulation broadly, and deepfakes specifically, posed to digital platforms. Key among these warnings were their placement within media and communication networks that allowed for

fallacies, conspiracy theories, and unvetted statements and events to proliferate among the online public — something that could, ostensibly, lead to political destabilization and violence at varying scales. And yet, while the hearing explored the possibility of violence as a result of deepfake deployment, very little time was spent on understanding the current reality of deepfake violence and proliferation as it is *now used* to target women, people of color, and other marginalized populations online, nor the systemic ontologies of the technology itself.

Deepfakes were treated as ontologically objective digital objects, unmoored from sociological biases and oppressions; informational weapons that could be used to exploit "psychological vulnerabilities" (ibid., 19) within the targeted population, while still being removed from any kind of definition of embodiment or identity — even though they are a technology that is, primarily, meant to algorithmically stitch and simulate the various experiences of embodiment.

Taking the aforementioned House Intelligence committee as emblematic of U.S. security trends in accessing, posturing and reacting to algorithmic media manipulation, this chapter argues, through an examination of deepfake trends that have gleaned attention in U.S. and international media, that the ways in which deepfakes are both future (security) risk and current (sexed, classed, raced, gendered) threat is rooted within gendered and racialized logics that, in turn, tie into their discursive and policy-oriented securitization.

Thus, the securitization of the deepfake within popular discourse is actually a securitization of the gendered and racialized digital body that is both othered and dissected within the deepfakes themselves. By considering how the deepfake works to securitize the body, I make the explicit argument that gender and racialization can help us speculate not only on the intricacies of subjects securitized online, but how said experiences create the conditions through

which a prosthetic securitization of the digital body becomes possible. That is, I consider: what logics create the conditions through which deepfakes are securitized prior to their actualization as a security threat, and how does the gendering and racialization of the bodies shown in these deepfakes — grafted, stitched, puppeteered and objectified — play into this?

The chapter begins with a brief discussion of focus and methodology, then moves on to an examination of the context in which the deepfake event exists, starting with the complications of digitalized embodiment. Intrinsic to an understanding of the ways in which we think about deepfakes — and about media manipulation and online identity in general — is an understanding of the gendered, racialized, and securitized environment of the internet, where specific forms of femininity, heternormativity, and prototypical whiteness form the basis of most peer-to-peer interactions, including the creation and spread of deepfake media.

I am interested in exploring the technological assemblage instantiated by the deepfake — one that combines artificial intelligence, online communication platforms, digital subjectivity, and security — and how said assemblage creates the conditions through which the digital body is made an object of violence. It is, of course, necessary to note that is it beyond the scope of this chapter to analyze all deepfakes or, for that matter, to argue for a hegemonic reading of the deepfake and its relationship to security, identity, and our online experiences.

Rather, I am using deepfakes as a laboratory for exploring securitized logics. In that vein, I focus my research and analysis on two case studies — two deepfakes events, really — that were given attention in both domestic U.S. and international Western media from November 2017 to March 2022. My methodology and focus is both on the technics of the content within these deepfakes — the kind of technological decisions and affects of these

decisions — as well as the discourse around them. First, I consider a professionally made campaign developed by ARS ELECTRONICA that features the face of former President Barack Obama and the voice of actor/comedian Jordan Peele as they warn against the dangers of fake news and misinformation as we attempt to reconcile the ways in which the PSA itself relies on racialized conceptions of national identity. Second, I highlight the role of deepfakes as a form of memefication within the space of international conflict, studying a viral deepfake meme of Russian President Vladimir Putin to understand how masculinity, violence, and the abject can be stitched into a digital body to perform what Jasbir K. Puar has famously termed homonationalism (Puar 2007).

Finally, I end by briefly exploring the infrastructural implications of deepfakes as a technology primarily used to abuse and control historically targeted populations online. Paralleling our discussion of deepfakes against the ways in which they are most widely made "viral" allows us to consider the place that deepfakes hold not just as an actualized form of digital violence and securitization, but as a media event and discursive trend. My analysis is an interpretative framing of themes, arguments, and focuses as they apply to deepfakes and similar technologies, enabling an interpretation of logics related to the technology, both on purpose and latent (Joffe and Yarley, 2004, 57).

Background and Method

While the salient threat of political destabilization via algorithmically manipulated media is not impossible, no such deepfake event has yet been launched targeting the United States and those that have entered into the international political milieu via online dissemination have met with limited success (Maddocks 2020; Simonite 2022). At the same time, deepfakes have

become commonplace in our daily lived experience, including — not unnotably — on some of the world's biggest pornography websites. In 2020, up to 1,000 deepfake videos were uploaded to porn sites every month, according to deepfake detection company Sensity (Burgess 2020). Similarly, deepfake detection software developer Deeptrace concluded in a 2019 report that out of a sample of almost 15,000 culled deepfake videos, 96 percent were pornographic, and 100 percent of pornographic deepfakes featured women, none of which were vetted for consent of the participants (Turk 2019). Indeed, deepfake pornography and deepfake-based sexual abuse has already been used to silence and discredit women and people of color from taking part in public forums online (ibid.).

And yet, while speakers at the U.S. House Intelligence Committee hearing briefly mentioned the disproportionate targeting of women and people of color by deepfakes, their discussion and scenario crafting primarily focused on threats to democracy via outside "adversaries" acting against an institution, in an apparent epistemological separation of the politics of securitization versus the politics of everyday gendered, racialized life (U.S. House Intelligence Committee, 40).

As journalist Victoria Turk put it, tongue firmly planted in cheek while writing in *Wired* on the lack of attention given to deepfake pornography and deepfake-based sexual abuse in the statements of public officials on the technology, "sure, deepfake pornography is bad, but hey, a fake-news deepfake of a politician could threaten the integrity of our democracy" (2019). Turk goes on to make clear that deepfakes of women *do* threaten the integrity of democracies — by silencing, humiliating and demeaning women. "When women's voices are silenced simply because they are women; when women are humiliated because they are women; when women are subjugated because they are women — these all pose a threat to democracy," Turk (2019)

continues, adding that securitized discourse around deepfake technology is not only astounding, but alarmingly off-point. “We have already seen real-world examples of deepfake pornography being used explicitly to silence and discredit women’s voices and prevent them from taking part in politics,” she writes (2019), such as in the case of former U.S. Rep. Katie Hill, who was victimized when sexual photographs were published of her in a right-wing media outlet without her permission. In a *Washington Post* piece on the incident, University of Miami School of Law Professor Mary Anne Franks (2019) notes misogyny intersecting with nonconsensual pornography is nothing novel but a tried and true form of “sexualized abuse most frequently directed at women who have committed the unpardonable sin of displeasing men” (2019).

It is in this apparent mismatch, between post-9/11 risk averse securitization logics that see new technologies as possible sites of unknown-unknown informational vulnerability (Amoore 2013), and the experiences of targeted populations online, that I base my inquiry. This chapter is interested in discussing why and how deepfakes can be both an issue of sexual violence and racism, and a matter of state security within the specific logics of digitalized and securitized embodiment. Deepfakes, as a technology, are seemingly chimerical — both imagined by security apparati as posing a *speculative threat* to national security while also having been proven, since their first appearance on the social media website Reddit in 2017 (Britt & Donovan 2019), to pose a very real danger for historically targeted populations who make themselves visible on digital platforms. Additionally, I am interested in the disconnect between what deepfakes do ontologically and their usage.

The case studies presented in this chapter highlight the ontology of the deepfake as a complex assemblage of dissected, stitched, violated, silenced, enhanced, slowed, sped up, and otherwise altered parts in contrast to their reception within the modern-day zeitgeist as a singular

object removed from the very bodies that make it up. Deepfakes represent a violent upheaval of previously normative assumptions about the authenticity of embodiment, identity, and information, creating the conditions through which digital embodiment itself is made violent.

Generally understood as videos created using a range of AI "deep learning" techniques to enable the manipulation of visual data, deepfakes are an intriguing (and emerging) area of research for several reasons. They are a relatively new instantiation of machine learning algorithms within the current online infrastructure. The first widely shared AI-manipulated videos appeared on Reddit in November 2017, when a group of users uploaded a batch of pornographic videos with the faces of female actors grafted onto other bodies (Britt & Donovan 2019, 5). In "The Word Real Is No Longer Real: Deepfakes, Gender, and the Challenges of AI-Altered Video," Wagner and Blewer (2019), explain that word "deepfake" is a catchy portmanteau of "deep (learning)" and fake (content)." Deep learning is best defined as the process by which a computer program repeats procedures rapidly, identifying patterns in order to generate new meanings. Ostensibly, it is artificial intelligence — a computer "learning" over time to generate new content based on information it is given (Wagner & Blewer 2019). And the more time and processing the computer has, the more realistic the deepfake will be.

It is important to note, as Paris and Donovan (2019) do in their *Data and Society* report "Deepfakes and Cheap Fakes," deepfakes live within a larger context — a field of audiovisual manipulation. "AV manipulation includes any sociotechnical means for influencing the interpretation of media. AV manipulation includes both the cutting edge, AI-reliant techniques of deepfakes, as well as 'cheap fakes' that use conventional techniques like speeding, slowing, cutting, re-staging, or –recontextualizing footage," they write (2019, 6-7). In this way, deepfakes can be reframed — from a blockbuster innovation somehow separated from daily lived

experience to a technological progression firmly rooted (or rather, stitched) within societal discourse, norms, habits and practices to simulate experiences or perspectives of embodiment.

Understanding deepfakes in this way allows us to more easily spot the nuanced — and critical — way this technology is changing our daily landscapes (online and off). For one, as Paris and Donovan (2019) write, deepfakes are applied to the *digitization of bodies*, including voices and likeness. The process can be completed with just a few hundred images, a bar many of us in the modern age — with our social media pages and mentions on websites — would easily meet. Secondly, deepfakes are distributed at lightning speed across all the platforms we're all on and also the ones we're not, making efforts to counter manipulation (or perhaps, most importantly, its negative impacts) all the more difficult (Paris & Donovan 2019).

To be sure, the deep-learning AI technologies behind deepfakes do not guarantee an inherently "unique" experience or contextualized product within the context of digital subjectivity and internet culture, but they do provide insight into trends in digital experience and discourse and, for purposes of broader inquiry, help us speculate on posthuman (perhaps even cyborgian) subjectivity. They are also (increasingly) easily accessible and programmable to those interested, with newer applications, such as Wombo.ai or ReFace, only requiring that users submit a photo and/or audio sample to upload. The ease at which these technologies can be accessed and used to disseminate altered visual media through state, institution, or individual, means that any output reaches larger scales at higher speeds, showing how the structural power of manipulators and users determine how media can be read as evidence that justifies physical, sexual, or political violence (ibid., 24). It is this very accessibility that has led some in the security sector to fear the deepfake as an informational weapon.

And yet despite the debate (and the stakes), deepfakes are currently woefully under-researched as digital objects and artifacts in and of themselves, even as they are over-represented in media and government documents as harbingers of a coming "information apocalypse" (Foe 2018; Chesney & Citron 2018; Gosse & Burkell 2020). Politicians, journalists, and others see deepfakes as having the unique ability to (all at once) tamper with elections, compromise national security, and encourage widespread violence, while media outlets claim that they will irrevocably blur the line between evidentiary and expressive video (Britt & Donovan 2019, 6). Worth noting: While this chapter does not wish to use deepfakes as a linchpin in any consideration of truth politics and digital media, popular coverage of deepfakes often sees "truth" in online media, or media generally, as stable — rather than determined in a (or any) way socially, politically, and culturally (ibid.). Extending this point of contention: Not all forms of manipulated visual media are "true" algorithmically manipulated deepfakes and yet, in popular discourse, deepfakes have come to represent not just the most technically sophisticated versions of the technology, but the most accessible and "cheapest" as well (ibid., 11). In line with Data & Society's research, this author seeks to keep deepfakes complicated, considering them on a spectrum — from those that require less expertise and fewer technical resources to those that require specific technologies and programming knowhow (ibid.).

Deepfakes: Secured, Embodied

In both media and in official government responses to deepfake technology, the conversation has been increasingly securitized. Here, securitization refers to — within discourse and zeitgeist — a focus on deepfake technologies as they apply to what are traditionally considered security, and not "normal" politics. As previously noted, securitization encompasses a

process where actants, such as the public, audiences, journalists, politicians, and others, come to a shared understanding around the perceived seriousness of a threat, as well as any subsequent push to "mobilize all … resources to curtail its development (Karyotis 2012, 391)."

Media plays a vital role in actuating this condition and while work on deepfakes and their sociological impact are still relatively recent, studies have found that deepfakes tend to be discussed in one of four ways:

- As being too accessible;
- As encouraging misinformation;
- As undermining the political process;
- And/or as non-consensual sexual content (Gosse & Burkell 2020).

Additionally, such coverage can highlight anxiety within the environment of media and journalism in and of itself, with some arguing that this relatively narrow bevy of perspectives reveals that 'journalists conjure up speculative worst-case scenarios around deepfakes to highlight the vital importance of journalism as a bulwark against fabrication and a defender of truth" (Wahl-Jorgensen & Carlson 2021). Regardless of the perspective(s) from which deepfakes are talked about in media and in public discussions, deepfakes themselves are most often considered either a tool of political subterfuge or a form of online abuse, representing a neutral social technology used by those with malintent, somehow, to silence critical speech (Maddocks 2020). In contrast, deepfakes are rarely considered a digital artifact representative of the ways in which sex, race, power, and security simultaneously creep into digital experiences of embodiment. In speaking of deepfakes as a form of embodied violence, we make the argument in this chapter that embodiment is more than just material.

Indeed, Laura Wilcox argues that by casting the body merely as material fact within studies of security, we limit our understanding of the "political possibilities" for different kinds of bodily politics (Wilcox 2015, 6). The "bodies" that exist within the context of any deepfake vary, both in their materiality (a pair of lips speaking words they never said; a head grafted, mathematically, onto the torso of another) and in their placement within any technological network. Put another way, they are, always already, a product and producer of a complex system of data, flesh and discourse. Deepfakes constitute a posthuman form of embodiment in which the body is constituted in and through violence. The violence of digital suturing, dismemberment, and objectification; the inherent violence of online gendering, racialization, and classism.

To be sure, securitization implies an understanding of the body as an individual organism whose protection from damage constitutes the provision — the necessity — for security (Wilcox 2015). This trend is paralleled within studies that attempt to critique security — with the people protected from violence, or who are killed or otherwise affected by Violence understood as only bodies. In such cases, the politics and sociality of bodies are erased (Wagner & Blewer 2019). For example, when deepfakes are discussed in the media, as in legislative sessions and hearings, the body is treated as an inert object that exists to be manipulated and not a material and discursive assemblage of flesh, technology, and law.

While this is largely ignored, these bodies are profoundly political, constituted in reference to historical political conditions while at the same time acting upon our world (Wilcox 2015). Violence, in this case, is a generative force, requiring us to pay attention to not just how bodies are injured as a result of deepfake proliferation and discourse, but how they enable, are formed, reformed, gendered, and racialized through political violence (ibid.)

Speaking of embodiment, I also turn to Judith Butler (2011) in this chapter to conceptualize the body, including the digital body, as performative. The digital body performs a narrativized reality within the deepfake it exists in — independent from and yet enabled by the material nature of its embodied components. Within this context, I consider both race and sexuality as technologies worked upon through the medium of the deepfake. I again echo Teresa de Lauretis' (1987) expansion of Michel Foucault, using deepfakes to work through how gender is carefully maintained and constructed as a product of social technologies and discourses, rather than a matter of sexual difference. Additionally, my conception of race as a technology is foregrounded by the work of Beth Coleman (2009), Lisa Nakamura (2002, 2007), and Wendy Hui Kyong Chun (2011b) in their consideration of online racial identity as a "carefully crafted, historically inflected system of mediation" (Chun 2011b, 28).

That the response to violence enacted upon and through a digital body depicted within a deepfake is latent securitization is no surprise when considering the nascent logic of securitization that defines the modern security state, especially in the context of the U.S. Indeed, a result of 21st century U.S. surveillance practices is that the term "security" and its offshoots has come to refer to a slew of requirements and parameters through which differences can be highlighted and dissolved at different times and places (Grewal 2017). Inderpal Grewal, in her examination of the security state, provides a broad definition of how security acts as a defining logic of 21st century neoliberal subjectivity. She writes, "Security… can also refer to the demands made on the state for safety and protection that it cannot ensure, and it often refuses to ensure. Security [and securitization] works through the promise of the safety of home and of nation, but also enables the powers of protection claimed by patriarchies, fraternities and nationalisms that work through violence" (2017, 13). It is within this context that

deepfakes become not just a product but an *actant* within securitization logics, artifacts exposing the ways in which heteronormative and racialized/racializing security extends online.

A President, A Comedian and Black Bodies

In February 2018, actor, comedian and director Jordan Peele collaborated with Buzzfeed, an American media company, to produce a deepfake in which President Barack Obama delivered a speech extolling the dangers of deepfakes as a technology. Peele's words and mouth movements were expertly stitched to Obama's face and likeness (Sosa 2018). The message delivered via this deepfake was similar to the line of questioning that would arise a year from its release at the 2019 Congressional Intelligence Hearing. Obama, in the video, is seen speaking the words as Jordan Peele's voice utters them: "We're entering an era in which our enemies can make anyone say anything at any point in time. They could have me say things like… Ben Carson is in the sunken place, or, how about this, simply: President Trump is a total and complete dipshit" (Sosa 2018).

The video is a bit of reflexive aesthetics, meant to bring awareness to the ease with which deepfakes create narrativized events and the susceptibility of online information (or, perhaps more accurately, the consumers of said information) to manipulation. Built using Adobe After Effects, a readily available video editing software program, and FakeApp, a desktop application that uses neural network technology to create deepfakes, the final rendering took 56 hours of automatic processing (Mack 2018). According to the programmers behind the deepfake, "Sosa first pasted Peele's mouth over Obama's, then replaced the former president's jawline with that moved with Peele's mouth movements. He then used FakeApp to smooth over and refine the footage" (ibid.) The PSA is a reference to prior cultural memes that give it a unique significance

to American audiences. Previously, Peele was known for his spot-on impression of President Obama, appearing often in comedy skits in the role of the President on skit comedy shows such as the Key and Peele show and Saturday Night Live, where he spoke in the President's distinctive accent and modeled his rhetoric. Among these skits were scenes in which Peele, acting as Obama, delivered a speech with his anger translator, Luther, played by actor Keegan Michael Key. While Peele's Obama was diplomatic and political neutral, Key's Luther interpreted his statements into angry, comedic statements that often directly referenced Islamophobia and racism in ways that Peele, as Obama, was unable to. For example, in reference to racially-charged conspiracy theories regarding Obama's birthplace, Luther ranted: "This is ridiculous. I have a birth certificate. ... I have a hot diggity, daggity, mama-sey mama sa ma-ma-kos-sa birth certificate you [expletive] crackers" (qtd. in Fresh Air 2015)

Obama's presidency was defined by a specific racial discourse shift in the U.S. Many declared the election of the first Black man as President definitive proof of America's racial progress, while others lamented the beginning of the end of (white) American exceptionalism (Guerrero 2016, 268). The birth of this so-called post-racial age was accompanied by an aggressive rebirth of race-based stereotypes, lexicons, and violent racist acts. The discourse of "post-racial" America resulted in communities of color, especially African Americans, simultaneously being cut off from claiming the significance of their racial identity, while still being defined by larger society through their race, which, allegedly, society had ceased to see (ibid. 269). It is into this racial milieu that Black satirists like Jordan Peele and Keegan Michael Key submitted their social commentary as comedy. "Key and Peele" began its five-season run in January 2012 as Barack Obama was running for his second term against Mitt Romney. As Lisa Guerrero (2016) explains in her work on comedy in Black America, "The country had been

deemed post-racial for almost four years, and the collective belief in the fantasy of an America beyond race had, in fact, generated a new American spectacle of race that reveled in both benign and base signs and images of race while supposedly remaining safe from the taint of racist intent" (269). Black satire worked, within this context, to locate Blackness and its meaning in post-racial America. Guerrero, examining performances such as those produced by Key and Peele, argues that Black satirists were (and are) essential knowledge-makers around the failures of the post-race myth, as well as the shifting precarity of Black subjectivity (ibid.).

For example, the skit that introduced Luther, Obama's "anger translator" later to be codified into the Buzzfeed produced deepfake, is a salient commentary on Black anger, in which Luther is presented through the lens of a legible imagined Blackness; bedecked with a "ring on every finger … he curses freely, gesticulates wildly and he breaks down… global and domestic politics through Black urban slang" (Guerrero, 270). Put another way, he is meant to portray Obama's Black conscious, the voice inside his head perhaps, embodying what are considered stereotypical signs of Blackness unavailable to Obama himself. This Cartesian perspective on Black masculinity — split, as it were, into a mind and body at odds — is made necessary because the performance of integrated Blackness is not allowed in the public sphere. An articulated Black rage, unremoved from the context in which it exists, works to unravel the myth of a post-racial United States. To Obama, Guerrero (2016) argues, Luther enacts the spectacular opportunity to bridge the split between mind and body — demanded of Black bodies in the United States — experiencing a temporary moment of integrated Blackness.

These performances, depicting the presidency at odds with the public performance of Blackness, are recreated in Buzzfeed's deepfake project. Indeed, the PSA is meant to remind viewers of the Luther sketches that first aired on "Key and Peele." Its central conceit is that

Obama, as president, politician and public figure, and as a Black man in a space traditionally afforded only to whiteness, would never say the things that he says. The message — that deepfakes create opportunities for the spread of misinformation and that public figures can be made to say things not in line with their public persona or roles (Romano 2018) — is only as effective as the cultural split between Peele's impression of Obama's famously even-keeled tone and the ways in which both he and the AI technology responsible for stitching together the body and voice of two Black men enact public Blackness through Obama's body.

It is this "spectacle of the other" (Hall 1997, 258), initiated through AI technology, that has the viewer gazing at a representation of others — via an imagined community of those who are "normal." In this instance, Blackness is a synthetic amalgamate, made to do the work of drawing a viewer's attention to something that does not belong; Peele's voice, references, and tone, coming out of Obama's body. That is, a Black man's voice — stereotyped and exaggerated in pursuit of satire — coming out of an American president's mouth. In the Buzzfeed sketch, Peele, as Obama, cautions viewers to "stay woke" (ibid.) so that we, as a culture, do not "become some kind of fucked-up dystopia" (ibid.) as deepfakes are poised to spread disinformation quickly and multi-laterally. The PSA's securitized message — indeed, a securitization of media consumption — is delivered by the simple act of Blackness as a racial technology. In other words, by thinking of race as a technology within a specific environment of techno-mediation, race itself works as a disruption that "changes the terms of engagement" within systems of representation and power (Coleman 2009, 178).

Race as technology

In her exploration of high-tech Orientalism in 1990s-era cyberpunk tropes, Wendy Hui-Kyong Chun (2011) argues the use of Asian imagery and aesthetics in creating futuristic dystopias was a paranoid reaction to global economic and data flows. It was these othered digital bodies that constituted race as a technology, allowing heteronormative whiteness to thrive in a hostile, culturally diverse space. This conceptualization suggests that race matters as a technology just as much when it is used to identify the hero as when it is used to visualize the subordinated other via stereotypical representations (ibid.).

Within this context, it is important to consider the ways in which Buzzfeed's Obama deepfake *itself* acts upon the racialized subjects encoded within its digital borders. While Jordan Peele's PSA is an enactment of Black satire, drawing our attention to the fallacy of a "race blind" America, the presentation of this message — and persona — via a deepfake is not without its nuances. Indeed, in this context, the digitally racialized Black body is subordinated to the performance of the presidency, where whiteness, and all its privileges, assumptions, stereotypes, and powers, are still the norm. This stitched representation — pathologization, really — of race is not just possible because of deepfake technology. It is integral to, and inherent of, deepfake technology *as it is securitized.*

Just as deepfakes are considered an informational weapon by public officials, the security apparatus, and media organizations, they also perpetuate state security as an *effect* (Gordon 1991) that aims to promise the safety of home and nation via colonial and racialized *affects* (Inderpal, 12). Deepfakes, via their internalization — that is, their uncanny ability to stitch together two characters, or bodies, or roles — call attention to the tensions that exist between race and national identity and how they can act as a form of social control and surveillance.

The profile of the adversary, the outsider, the outlier, or the other, however, is dynamic and ever-changing, formed out of ever-shifting concepts of racialized fear and information flows, which are — in themselves — identified by religious, gendered, and racial characteristics produced by histories of imperialism and colonialism. Indeed, as Foucault (1995) argues, racialization and racism introduce a break into the domain of life that is under power's control: the break between "what must live and what must die" (Foucault 1995, 254). This death is not only literal but "every form of indirect murder: the fact of exposing someone to death, increasing the risk of death for some people, or … political death, expulsion, rejection and so on" (ibid.).

This postulate, applied to the Buzzfeed PSA, illuminates the (again) literal and allegorical/imaginary death/erasure of the Black man in subordination of the role of the U.S. presidency via deepfake protocols, helping us consider how the construction of a domestic mythos of American national identity is produced and mediated around a racialized, othering logic. Indeed, Guerrero (2016) writes eloquently on the power and promise of Black satire in illuminating the absence of African Americans from postmodern theory, noting the experiences of Black Americans in capitalism and humanism — in stark contrast to white Americans — have been undergirded by profoundly violent power structures. She continues:

> Within the system of US capitalism, African Americans' role has been as human commodity, cultural commodity, and exploited social class, all of which are crucial components of the capitalist system, just not socially equal ones. Similarly, African Americans' claim to liberal humanism, an ideology that proposes that the essence of man is freedom and that the subject is the liberated creator of both meaning and action, has been limited and oftentimes outright prohibited. This ideological prohibition makes African American efforts toward freedom, as both citizen and subject, a differentiated proposition from those whose humanity and subjectivity are naturalized. (2016, 267).

Put another way, Guerrero concludes, capitalism *happens* to African Americans even as a full claim to liberal humanism is denied them, making Peele's "anger translator" a potent social critique made all the more jarring by deepfake technology — with its stitched bodies — and a

point of knowledge making, underscoring saliently the failures of the post-race myth (Guerrero 2016). In this way, the comedians Key and Peele go beyond simply blurring the "ideological boundaries of Blackness" to doing away with them altogether, engaging in Lyotard's "inventor's paralogy" (ibid.) as they locate themselves through difference and seek to replace actual experiences with reflections of Black stereotypes in the national consciousness.

Is it me? Am I The Problem? War, Masculinity, and Putin, Deepfaked

In the Spring of 2022, shortly after Russia's brutal invasion of Ukraine began, a deepfake video depicting Russian President Vladimir Putin recreating a popular TikTok meme went (not surprisingly) viral on the platform. In the video, now viewed at least 123 million times on TikTok alone, Putin is shown smirking almost coquettishly at the camera. His lips move and the voice of Scarlet Envy, an American drag queen who was at the time competing on the reality TV show "Ru Paul's Drag Race All Stars" Season 6, is heard as a deepfaked Putin opens his mouth: "Is it me?" Putin says, uncharacteristically wagging his head back and forth. Putin as Scarlet Envy continues: "Is it me? Am I the drama? I don't think I'm the drama! ... Maybe I am. Am I the villain? I don't think I'm the villain."

Created using Wombo.ai, an easily accessible app through which users submit video and voice clips to create mash-ups of public figures and audio clips, the post was but one among countless memes of Putin created and disseminated on Tiktok and other social media platforms during the first six months of the Ukraine-Russian conflict. In fact, the sea of war-related posts was so vast, the *New Yorker* dubbed it the "first TikTok war" — gruesome images of battle, missiles raining down on cities and towns, the funny, odd and mundane that still somehow happens amid the frenzied chaos of conflict were all captured with smartphones and uploaded to

the platform with a pace and at a volume not seen before (Chayka 2022). “It is surreal to see well-established social-media formulas applied to ground warfare. …. The flood of TikTok videos … perhaps more likely to evoke our bemused awareness, a feeling of sympathy that lasts only long enough to keep us scrolling,” Kyle Chayka (2022) writes, in *The New Yorker,* pointing as an exemplar to a February 12th post of a Ukrainian solder in uniform moonwalking to “Smooth Criminal” in an empty field. The post garnered twelve million likes and hundreds of thousands of comments, including “be safe guys.”

It is in this digital landscape (both bizarre and familiar to many of us) that the Putin-as-Scarlet Envy deepfake was dropped — not by any means convincing as an actual video and certainly not meant to be. Rather than deceiving viewers, the Putin-as-Scarlet Envy deepfake offers a wink-wink moment of fun, all at once lampooning Putin, his government and his policies from a particularly Western perspective. It also deploys a visual intervention in international politics that can be considered a noteworthy extension of the iconic Gay Clown Putin meme (Cooper-Cunningham 2022), which plays satirically with Russian political homophobia and security via a purposefully queered perspective.

A Gay Clown Putin is Born

As Cooper-Cunningham (2022) explains, the Gay Clown Putin meme is a powerful, multi-platform trend seen around the globe that explicitly targets Russia’s homophobic domestic politics as the subject of critique. Backgrounding the meme: relentless oppression and persecution of LGBT people via a “state-directed political homophobia” that justifies fears of gender and sexual expression outside of heteronormative/patriarchal structures as a national security threat emanating from the West (Cooper-Cunningham 2022). The homophobic

propaganda is woven seamlessly into Russia's broader nationalist platform and its embrace of machismo and masculinity — a process characterized as the "remasculation of the nation" (Riabov & Riabova 2014) and achieved by promoting (hyper)masculine imagery and ideas of the nation while simultaneously demasculinizing others. Case in point, Slootmaeckers notes, is the "Gayropa" trope — meant to denigrate Western acceptance of homosexuality.

Given the givens, there's little wonder why the Gay Clown Putin meme almost instantaneously gained traction. Its roots in international visual discourse can be traced to 2013, when Russia enacted its "gay propaganda" law, banning the "promotion … of "non-traditional" sexuality and/or gender to minors (ibid.). Putin's Russia justified the "gay propaganda" law by arguing queer individuals constituted a threat to the "traditional Christian values" underpinning Russian civilization (Cooper-Cunningham 2022). Before the Russian invasion of Ukraine, European states implored Russia to follow their (not without flaws) lead by broadening and strengthening key legal protections for LGBT people — a political movement Russia characterized as encroaching on its sovereignty (ibid).

Following passage of the "gay propaganda law," Dutch LGBT rights organization COC Nederland launched putinarainbow.com, a website that playfully invited people to upload images of Putin with rainbows incorporated into them (Cooper-Cunningham 2022). Since the campaign's launch, graphical depictions of Putin with rainbows have been used prominently in myriad protests of Russian policies, including demonstrations against the Sochi Winter Olympics. Gay Clown Trump and Gay Clown Orban, depicting Hungarian Prime Minister Viktor Orba, have also been used as cogent statements in political rallies. As Cooper-Cunningham writes, Gay Clown Putin speaks to Putin's own policies and the central political platform in Russia that concludes queerness poses a "internal security threat" — and amounts to

Western subjugation (2022, 307). Here, "security" in the Russian view emerges as a discursive practice, modeling the Other's difference as threat in a useful way so as to at once suppress particular groups of people while establishing the superiority of the Self (Hansen 2006).

Putin, Re(de-)skinned

To make a finer point of it, as Cooper-Cunningham (2022) do, Russia's construction of queerness as national security threat not only establishes heteronormativity/heterosexuality as superior but establishes it as *Russian*. It is for this reason precisely that the Putin-Scarlet Envy video is illuminating in a discussion on deepfakes as technologies of securitization. On its face, the eight-second video is part of an oft-played othering via emasculation on the international stage. Putin as Scarlet Envy is placed in sharp contrast from the hypermasculine Putin the world seems to know; the Putin who invades neighboring countries, disappears political dissidents and abolishes LGBT rights. With a drag queen persona, Putin offers playful dialogue and facial movements — tropes lampooned as *othered queer*. In "Rewriting the stars: Surface tensions and gender troubles in the online media production of digital deepfakes," Holliday (2021) considers this kind of "reskinning" of cisgender white males in a series of deepfakes featuring Hollywood stars, noting how the digital creations sharpen the ontology of gender as understood through discourses of performativity (*a la Butler*) that identify masculinity as a series of embodied practices — repeated acts, for example, or gestures. Here, deepfakes allow for fictional domains that "ramify from the actual state of affairs" (Ronen 1994, 199), creating spaces for intertextual meaning-making via bodies that are switched, stitched, exchanged and modified.

Substituting Putin with a drag queen is not *inherently* a defiant act — just as drag itself is not born rebellious (Buttler 2014), even with its (pre-)occupation of a space that looks to

annihilate ideals of gender. However, drag in this context is critical, offering space for a parody of masculinity and gender even as it tacitly reasserts gender norms with its juxtaposition of Putin with Scarlet Envy. Critical Camp scholarship further elaborates on this point, offering a lens through which to understand drag's role in the 21st Century as a performative act, further revealing how identities are fundamentally social constructs — solidified by repetitious actions (Schotmiller 2019) — but also as a queer ideology. In other words, the very intentional use of drag in the Putin-Scarlet Envy deepfake acts subversively even as it is reiterative (Holliday 2021), offering a fluidity to the viewer that is both human and machine. As Holliday posits, "As a performance that makes gender a spectacle (and a problem) of technology, all deepfakes solidify and displace the reality and artifice of gender, both at once. They are forms of 'digital drag' because they occupy precisely this middle ground, undoing gender while also reiterating its signifiers through the combination (and rewriting) of stars" (2021).

The Emperor Has New Skin

As Cooper-Cunningham (2022) writes, visual memes as political intervention and discourse are, simply put, complicated — multi-faceted, multi-layered and deployed, contextualized and interpreted differently. Thus, the Putin-Scarlet Envy video — while relying on stereotyping assumptions and othering discourse — also/at once uses a digitally embodied form of the abject as a productive critique of heteronormativity in a way made uniquely possible by the body-stitching technology of deepfake videos.

In doing so, the meme expertly highlights the importance of gender — and especially particular definitions of masculinity — in international conflict. Indeed, the role of (hyper-)masculinity in global conflict and, more broadly, modern nationalism cannot be overstated.

Slootmaeckers (2019) writes eloquently on this, developing a feminist theoretical framework that places masculinity and nationalism on "two sides of the same coin" — the central difference between them being the deployment of homophobia as a "technology of othering within different types of self/other relations" (239).

Similarly, understanding heteronormativity as inherently political offers a critical lens with which to consider deepfake discourse broadly — and the Putin-Scarlet video in particular. Here, Putin's own political machinations of LGBTQ othering are laid squarely on his own persona, critiquing not only his homophobic platforms but his invasion of Ukraine under the guise of nationalist pride and grievance settling.

Anderson (1991) points to the gendered structure of nationalism and boundary construction as an exercise in othering, making clear that the discourse of nationalism is never just about what (or who) is within a country but is inherently international, designating and assimilating "insiders" and/or "citizens" while rejecting, excluding and dehumanizing those labeled "outsiders."

Slootmaecker (2019) writes, turning to Foucault, nationalism's core technologies of othering are inherently gendered and fundamentally destructive, relying on patriarchal tropes and assumptions about labor, worth, and societal value. In the case of the Scarlet Envy-Putin video, an analysis of hegemonic structures of nationalism and masculinity draws our attention to the political nature of othering — which reduces people to objects/abjects, used, discarded or destroyed (Slootmaeckers 2019). When Putin's body is stitched to Scarlet Envy's voice, suddenly, the violence in nationalist masculinity is laid *more* bare, offering a critique that is reminiscent of Puar's theory of homonationalism — by which (some) homosexual bodies are "worthy of protection by nation-states" (Slootmaeckers 2019, 256). As with Gay Clown Putin,

the context is key: Memes proliferating in the Western world take aim at practices elsewhere, defining insiders as enlightened or progressive while painting outsiders as backwards. This boundary drawing sets up what Slootmaeckers (2019) dubs a process of competing masculinities, constructing national boundaries using masculine othering based on a "logic of contrast." "Here," Slootmaeckers (2019, 252) suggests, "nationalism confirms the superiority of the nation by comparing it to other nations, which are deemed to be masculine yet inferior in their expressions of masculinity." Intentionality aside, these mechanisms are at play in the Putin as Scarlet Envy deepfake; in the shadows — behind its work of embracing queerness and lampooning it — the depiction sets up a homonationalist framework that contrasts *them* and *us*.

Conclusion: 'An Illusion' and Opportunities for Future Study

Phillip K. Dick's *Minority Report* explores identity as an issue of agency and free will against the iffy standardization of pre-emptive policing. In the film by the same name, John Anderton, after he (eventually) murders Leopold Kaplan, realizes that the complexities of the precog system — an assemblage of three "gibbering, fumbling creatures" that tell the future — are such that any suspect-finding via the system is in danger of being an illusion based on positive data input. In his words, "That's all it was, an illusion." An illusion much like Guattari's faciality of reference and the projection qualities of faces of authority (Deleuze and Guattari 2004). Faciality considers the social, technical, and aesthetic mechanisms that organize embodiment and subjectification via the face. According to Guattari, the face has become a frozen Western culture — there is a disconnect between surface "features" and the "mind" behind them. Indeed, interfaces force constant face-to-face relations with computers, either by standardization via computational logics or by providing machines with a "human face."

Interesting to note, however, is that these facilities, and mechanisms thereof, are constantly coalescing and morphing into strange (science fiction-esque) worlds. Case in point: AVATAR (Automated Virtual Agent for Truth Assessments in Real Time), as detailed in Chapter Two, is an AI kiosk meant to replace the border agent. Programmed to "detect deception," AVATAR resembles an ATM, with cameras and microphones and scanners meant to create a biometric read-out of an interviewees embodied data. It also has a face — a computer-generated Caucasian male quizzes potential travelers, wearing a tidy white Oxford shirt and tie. AVATAR's … avatar exists as a face to be watched, studied, and interfaced with, as a facial reference meant to enact some kind of hierarchy between machine and individual and, according to its designers, represents the "personification of the system." AVATAR, if anything, comes

close to being a literal capitalistic faciality machine, merging the spectacle of the face, with the interfacial standardization of computation. The face here, in both the case of "Minority Report's" Anderton and AVATAR, is not just a node of relation between subject and authority but a projection of accepted embodiment onto an audience. In other words, "it is an illusion" — meant to trick and convince while ultimately interacting with humans in particular ways.

In this brief conclusion, my aim is to offer potential opportunities forward in the domains of study undergirding the cases explored in this dissertation. The lightning-fast advancements in relevant technology mean these areas of critical research are ripe for expansion. First, however, I will consider a politics of refusal in the face (pun very much intended) of pervasive embodied capture within the machine, paying special attention to current discourse as it applies to modern conceptions of both privacy and resistance. Specifically, I will unpack surveillance in society, privacy and resistance — all within the context of the ground I have already covered in Chapters Two through Four. Finally, I will seek to notate the limitations of my own research as I point to potential areas of future study.

'A Field of Visibility'

Surveillance is the idea that real people are watched doing real things, unknowingly. David Lyon (2015), for example, describes it as "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered." To be sure, Lyon's understanding of modern or liquid surveillance should be understood more in the context of function creep than it should in the context of Jeremy Bentham's panopticon (i.e.: the rigid tree versus creeping vines metaphor). Michel Foucault (1995) first suggested the potential for surveillance to be used as a technology of statecraft in "Discipline and Punish," positing it could produce more docile bodies — essential to state

functioning. He noted, especially, that the state-as-surveillance could not only be a form of external policing but also a potent means of creating internalized systems through which subjects would then police themselves. As Foucault wrote, “He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation which simultaneously plays both roles; he becomes the principle of his own subjection” (qtd. in Bauman & Lyon 2013, 13). This theory of self-policing is captured in Jeremy Bentham’s panopticon metaphor — an architectural concept/structure in which prisoners are clustered around a guard tower that may or may not have a guard in it. Regardless of any actual surveillance, these prisoners always behave as if under surveillance because of the possibility that they may be watched, changing their behavior due to an invisible transcendent scrutiny (Dubrofsky & Magnet 2015).

The surveillance applications of AVATAR at the “e-border” make this clear, presenting a digitized proxy of the sovereign state by facializing subjectification, emulating authentic human intersection to exert biometric discipline and control. And just as in the panopticon, subjects can find themselves becoming complicit in their own domination, recognizing the designated authority and purpose of the “conversational agent,” programmed and presented to treat the individual as object through which/on which power is applied.

To be sure, in surveillance studies the adaptability and applicability of the panopticon has made it something of a favorite meme. Benjamin Bratton (2016), for instance, speaks of an inverse panopticon in “The Stack.” There are electric panopticons and superpanopticons, synopticons and polyopticons (Bauman & Lyon 2013). There are even post-panopticons. But beware here: The imagery of the panopticon can create a paradox (ibid). To visualize this paradox, consider the differences between the way studies focusing on either “hard” or “soft”

forms of surveillance approach the idea of the panopticon. Lorna Rhode shows us that the supermax experience pushes some inmates to self-mutilate as a calculated manipulation against negative visibility (Bauman & Lyon 2013). Similarly, the panopticon in the consumer context is used to argue that any panoptic power is commodified, intent on "lulling and luring the unwary" (Bauman & Lyon 2013).

So on one hand, you have moments that generate a kind of resistance against the ontological subjection of the docile body. On the other, you have a seduction of the unknowing subject into a commodified and entertaining conformity. How might we see our digital friend Tay.AI in this context? The Microsoft chatbot, as detailed in Chapter Three, was programmed to impersonate a young adult woman, ready to play games and share horoscopes, but quickly devolved into tweeting "wildly inappropriate" responses, even repeating a neo-Nazi pledge. In detailing the embarrassing episode and its foundational implications, I argued that Tay.AI's dark metamorphosis had everything to do with how race, gender and class operate as technologies themselves — reproducing themselves in the digital.

At the same time, an application of the concept of liquid surveillance (Bauman & Lyon 2012) is helpful here in (re-)envisioning the panopticon where Tay.AI exists as less a parallel to liquid modernity and more an aspect of it, working in concert with the function creep of consumer data collection and visibility to augment and personalize state control. Tay's design flaws allowed and/or compelled the chatbot to mimic sexually abusive, racist and misogynistic messages, turning AI monster both because of a failure of computational programming — falling prey to the worst tendencies of internet trolls — and a failure of gender and racial programming.

In this way, we can see how liquid surveillance was both built into the system and prescribed for the system — the result a reflection of the othering, racist and discursive practices

that are replicated in and by hegemonic structures that exert power in the post-panopticon (Bauman and Lyon 2012). Put another way, Tay.AI is a product and a producer of liquid surveillance — each part interplaying in the digitized context. Perhaps most tellingly, Tay.AI's monster-ification demonstrates the insidiousness and apparent invisibility of liquid surveillance and its "mobile, pulsating signals of today's flowing forms" (15). Tay.AI was subverted by willing participants in just a day, the resulting chatbot tweeting feverishly before being dismantled. As Bauman says in his "conversation" with Lyon, "everything moves from enforcement to temptation and seduction" (57). In other words, the surveillance society no longer needs victims because it has volunteers.

As such, Bauman and Lyon argue, modern surveillance primarily serves as a "social sorting" or, as Gandy (2009) puts it, constructing a world of "cumulative disadvantage." That "social sorting" is visible, too, in the deepfakes taken up in this study. Obama's "anger translator" is a potent "reskinning" of a man the entire world is familiar with. Here, we can see surveillance at work in asserting questions about what it means to be Black in the United States and to be the president of the United States — and, indeed, to be both. Even as the satirical deepfake questions "race blind" America, it reinforces an America where whiteness is still the norm, using a popular comedian and the former president to tell the story. To further unpack the Obama-"anger translator" deepfake, we might turn to the notion of the "synopticon" (Mathiesen 1997), in which the many watch the few — a salient model of surveillance in a consumer society. Meanwhile, the second deepfake taken up in Chapter Four, that of Putin-as-Scarlet Envy, additionally demonstrates a salient critique of the "ban-optican" — that is, profiling technologies used to determine specific groups to place under surveillance — even as it

demonstrates the power of liquid surveillance as less of a categorization or specification of surveillance and more of an orientation.

To be sure, the kind of power asserted through digital technologies like deepfakes, applied in the mutable societies of control Deleuze envisioned (1992), does not fit into the walls and windows of the panopticon (or, for that matter, many of its cousins). These assemblages have no general connection with imprisonment; instead, they're marketed as being about flexibility, efficiency, or entertainment. Function creep — and the characterization of surveillance as liquid — describes more the modern security-imperative of pre-emption and future-oriented thinking. In this way, surveillance is understood as part of a temporally-in-flux, interconnected network. Additionally, the concept of liquid surveillance helps in orienting us toward a new understanding of privacy — elucidating the highly mobile, adaptable and diverse ways in which personal data is collected (though content creation platforms and much more), raising the stakes for how and why any kind of resistance, or refusal, is necessary, and prompting questions about how (and why) privacy is the concept through which to think through that refusal (Bauman & Lyon 2013). In terms of the ethical responsibilities of any study on surveillance and the body, then, it is necessary to focus on how modern surveillance techniques augment the sociopolitical environment in a way that resonates with norms and values. That is to say: In a study on any type of data collection or surveillance, discussing it in the context of privacy is almost a programmatic imperative.

Privacy: Politics of Sight

The loss of privacy in individual lives — and intrusion of state-based entities (or, the possibility of that intrusion) — is a very real problematic and critique, analysis, and

dissemination of the strategies and tactics used by hegemonic powers to surveil is a salient conception, and validation, of subject agency in the face of social control and identity standardization. At the same time, as Charlotte Epstein argues, privacy is political (2016). Centering discussions of surveillance on its relation to conceptions of the neoliberal subject's right to privacy both creates and obfuscates possible avenues of analysis, response, resistance, and/or refusal. The diffusion of surveillance technologies through our everyday lives, increasingly, problematizes the distinction between public and private (Epstein 2016).

Backgrounding Chapter Two's discussion of AVATAR is a rich debate around securitization, surveillance and privacy. As discussed, AVATAR digitally dissects the body and facializes the subjectification process as it serves as a proxy sovereign. Especially in the increasing prevalence of biometrics, as with AVATAR, the body is what's at stake; both in terms of how state/citizen relationships are shifting under the conditions of modern surveillance and in debates concerning privacy and data protection. To be sure, the discourse surrounding privacy is deeply ambivalent. Privacy has been extensively critiqued as a Western liberal conceit, as in Benjamin Bratton's analysis in "The Stack" (2015), where he argues that the "Oedipal discourse of privacy and transparency" is necessary but has real limits.

Specifically, he writes, a politics of computation predicated on the biopolitics of privacy, of "self-immunization from any compulsory appearance in front of publics … can sometimes serve as an internalization of the neoliberal subject (ibid. 60). It has done little, as well, as a tactic against the expansion of surveillance. Similarly, Rachel Hall shows in her article on full-body scanners in U.S. airports that privacy concerns have not kept vulnerable communities safe from invasive pat-downs and biometric identification, begging the question: Who has the right to privacy? And how is privacy politically situated within systems of control and institutionalized

racism, sexism, and othering? Indeed, what type of sociopolitical positioning does it require to be able to afford something like encryption or opacity (Dubrofsky & Magnet 2015)?

Yet privacy is recognized as an international right (via Article 17 of the 1966 International Covenant on Civil and Political Rights) and defended as a requirement of modern democracy. Colin Bennet argues that as a concept, an instrument of policy making, and a way to frame activism, privacy is not going to disappear (Epstein 2016). Indicative of this necessary turn toward privacy are sharp critiques of intrusive transgressions. Case in point: The Perpetual Lineup, a project and website run by Georgetown's Center on Privacy Technology that uses data gleaned from public record requests to track unregulated use by state and local police departments of facial recognition databases. At stake here, just as with AVATAR, are the risks facial recognition databases create for "privacy, civil liberties, and civil rights" (ibid). TPL works within a normative understanding of surveillance, law enforcement, and the juridical system, applying the U.S. legal framework of the 4th and 5th Amendments in a bid to define proper and improper uses of face recognition. To this ouroboros of privacy — where it is alternatively rejected and simultaneously held up as a benchmark of democracy and liberalism — Epstein (2016) suggests a shift to the language of the embodied subject. Via an understanding of Hobbes' "in secret free," she argues that personal, embodied freedoms and privacy have been interconnected since the beginning of the modern security state. Here, she continues, is where the attachment to privacy originates; as a cornerstone to a subject's agency and as an attachment to the old regime of sovereignty.

Feminist surveillance studies can further elucidate this point, questioning the very foundations of "scientific neutrality" and "bureaucratic record keeping" — as has been presented with such technologies as AVATAR — as a way of interrogating modern conversations of

freedom, privacy and surveillance. “All forms of data collection have imperatives built in,” Andrejevic (2015, xiii) writes, adding there is power in critically “disembedding and exposing these imperatives, the interests they serve and the uses they enable.” Take data mining, for example, considered by many to be devoid of identifying attributes and information in its “purest” form — free from subjectivity or discrimination. You need only look for discrimination in data mining to find that it is there — hidden in the decisions about disagreegation of data sets, how data is finely sliced, and finally, how it is presented (Andrejevic 2015). Shoshana Magnet expertly expounds on this academic area of study, demonstrating how biometric technologies, biases, preconceptions and prejudices can be “baked into code, where they continue to operate in opaque ways” (Andrejevic 2015, xv).

Something to hide

These “in plain sight” code assemblages were also baked into Tay.AI — a (feminine) chatbot built for polite, trendy conversations that quickly devolved into neo-Nazi rhetoric. Tay.AI not only understood its audience — it expertly mimicked them, mining into their digital profiles and into its own code to understand who it needed to be as it assimilated into their world — just as the facial recognition technology programmed into AVATAR is codified with preconceptions about gender and race from the beginning (Andrejevic 2015). As Andrejevic writes, the biggest clue about these processes at work comes in the difficulty that algorithms have in predicting what counts as rare and exceptional occurrences. “That is to say,” he continues, “historical understandings of what is ‘to be expected’ have a way of working themselves into the algorithm” (Andrejevic 2015, xv).

It is in this context that the Googles and the Facebooks and the CIAs of the world operate, blithely swiping away privacy concerns by at once arguing that surveillance technologies are inherently objective while also suggesting that the abstract "we" have the best interests of the securitized state — and thus civil society writ large — in mind. There is an obliviousness here, too, to non-white, non-heteronormative experiences. Otherwise, how could the CEO of Google ever utter these words — "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place" (qtd. in Metz 2009) — with a straight face? Of course, a wealthy, cisgender, white, American CEO needn't worry about monitoring practices — including those he himself benefits from — and of course, he has no conception about the lives of those who might, both in the United States and around the globe. Alarmingly, his statement not only ferrets away suggestions that technological erosions of privacy are suspect or problematic, it also suggests that those who face threats of discrimination, exploitation or exclusion have "something to hide." If they suffer some ill effects from those same technological assemblages, so his thinking goes, they must have deserved it.

A clear example of the intrusions and violence of technological assemblages on privacy can undoubtedly be found in the world of deepfakes, discussed via two case studies in Chapter Four. Noted in my analysis, but not unpacked in any thorough way and certainly an area rife with possibility for scholarly research, was the proliferation of deepfake pornography, much of which includes nonconsensual imagery. To be sure, this is an emerging area of academic work, but feminist frameworks offer a solid foundation from which to approach the topic.

As deepfake detection company Sensity reports, deepfake pornography is "by far the most prevalent kind of deepfake being circulated (Ajder et al. 2019). In fact, one report in 2020 put the figure at 96% (Burgess 2020). Put another way, more than 9 in 10 deepfakes crafted,

disseminated and shared online are pornographic in nature with dubious or nonexistent norms for consensuality. To those familiar with deepfakes, this was not a surprise. Indeed, the first widely shared deepfakes were pornographic, depicting the faces of actresses grafted onto bodies engaged in sexual acts (Cole 2018). Since then, deepfakes have become commonplace on some of the world's most accessed pornography websites (Turk, 2019). Deepfake pornography videos, hosted on three of the biggest porn websites, XVideos, Xnxx, and XHamster, have been viewed millions of times, and include both celebrity and non-celebrity faces grafted onto the bodies of actors and actresses having sex (Burgess 2020). The full scale of deepfake porn is unknown — some videos, but not all, include the words "fake" or "deepfake" in their title, making the process of identification unclear.

Additionally, companies that focus on porn and sex work, such as those listed above, do not currently have deepfake-specific policies or education. xHamster's moderation process, for instance, involves multiple steps that will remove videos if an individual's image is used without permission. However, deepfake porn is removed not as a possible act of inherent sexual abuse, but as a violation of the websites Terms of Use (ibid.). In some instances, banning deepfakes has proven of little use, as with Pornhub, which still sees a significant number of celebrity deepfakes uploaded (Rinelli 2023). Furthermore, legal options for those featured in deepfakes are limited, or at times completely unfeasible — ranging from defamation to copyright complaints with no set deepfake-specific strategy.

Deepfakes present a very real problem for women and minorities online, despite being a relatively recent disseminated technology. As Sophie Maddocks writes in her examination of feminist activism in response to non-consensual pornography (or NCP), porn is both industry and idiom, referring to both a trans-national corporate industry and a revealing discourse on social

norms, taboos, and the abject (Maddocks 2021, 5). Many scholars and activists have pointed to pornography's therapeutic potential (Lane 2012, 165), its usefulness as a tool for sex education (Penley 2012, 195), as well as its place in reimagining sexual politics and diverse sexual subjectivities (ibid.). While there is potential for liberatory pornography, much of mainstream porn reproduces stereotypical and consumptive logics of sexuality (Franks 2006). The reification of these logics is further complicated when considering deepfakes and their relationship with consent, sexual abuse, and exploitation.

The Limits of Invisibility

At the same time, we must be cognizant that modern notions of privacy — an heirloom of historical reactions to sovereign power — are a social construction networked through subjectified autonomy and opacity. Here, we might beg the question: Does opacity, or invisibility, or non-visibility, guarantee a kind of freedom? Is the distinction between freedom and subjectification as clear cut as not being seen? As Bratton (2015) writes: "The automatic narcissism [of privacy via the neoliberal subject] means that the world endangers you; the empire cares about you, who are such an important threat to the order … this glass of immurement calls for absolute transparency when looking up and absolute opacity when looking down, but it is never so clear where we are, even if we are within an architecture with clear directions of stratification in the first place."

In thinking through privacy in liquid modernity, then, where function creep and oscillating individual power dynamics, control, and agency interact, it is critical to take note that the politics of sight are never so binary. Indeed, as Timothy Pachirat (2011) reveals in "Every 12 Seconds", an ethnography following the work that goes into an industrial slaughterhouse, a more

nuanced relationship exists between sight and concealment than the binaries between visible/invisible, plain/hidden, and open/confined. Making the hidden visible, he finds, (in speaking of the spatialized methods of surveillance and management that go into the work of killing) is just as likely to generate more effective ways of confinement.

Pachirat's research, and Bratton's critique of the private neoliberal subject, beg the question of how privacy and confinement are not inherently the tools of a subject seeking autonomy and freedom outside the eye of the sovereign. Just as much at stake — the ways in which opacity and confinement itself cauterizes and self-immunizes from any public accountability. And in a culture saturated (and to an extent formed by) social media — like the Putin as Scarlet Envy deepfake discussed in Chapter Four — many of us want to see and want to be seen; the kinds of validation offered by networks of visibility, and the self-branding/online curating required by the modern job market, make problematic a certain degree of privacy right at the get-go (Marx 2016). That is to say that while advocating for non-visibility offers a powerful response and rejection to the growth of state control via data collection and subsequent knowledge of the (digital) embodied subject, it is not without its problematics and contradictions. Gary Marx, in his examination of these issues and counter-issues, suggests (tongue firmly placed in cheek) we look at surveillance and its opposites not through the model of the panopticon or utopicon, but the perhapsicon; "Perhaps, sometimes, perhaps even often, but sometimes never, and in addition, make room for counter evidence, conflicting values and outcomes and new factors" (2016, 308). In examining surveillance, the thinking goes, a mode of analysis less bent on visibility/invisibility binaries could tease out some new ways of thinking through autonomy, power, control, and the body. we must be cognizant that modern notions of privacy — an heirloom of historical reactions to sovereign power — are a social construction networked

through subjectified autonomy and opacity. Here, we might beg the question: Does opacity, or invisibility, or non-visibility, guarantee a kind of freedom? Is the distinction between freedom and subjectification as clear cut as not being seen? As Bratton (2015) writes: "The automatic narcissism [of privacy via the neoliberal subject] means that the world endangers you; the empire cares about you, who are such an important threat to the order … this glass of immurement calls for absolute transparency when looking up and absolute opacity when looking down, but it is never so clear where we are, even if we are within an architecture with clear directions of stratification in the first place."

In thinking through privacy in liquid modernity, then, where function creep and oscillating individual power dynamics, control, and agency interact, it is critical to take note that the politics of sight are never so binary.

And in a culture saturated (and to an extent formed by) social media — like the Putin as Scarlet Envy deepfake discussed in Chapter Four — many of us want to see and want to be seen; the kinds of validation offered by networks of visibility, and the self-branding/online curating required by the modern job market, make problematic a certain degree of privacy right at the get-go (Marx 2016). That is to say that while advocating for non-visibility offers a powerful response and rejection to the growth of state control via data collection and subsequent knowledge of the (digital) embodied subject, it is not without its problematics and contradictions. Gary Marx, in his examination of these issues and counter-issues, suggests (tongue firmly placed in cheek) we look at surveillance and its opposites not through the model of the panopticon or utopicon, but the perhapsicon; "Perhaps, sometimes, perhaps even often, but sometimes never, and in addition, make room for counter evidence, conflicting values and outcomes and new factors" (2016, 308). In examining surveillance, the thinking goes, a mode of analysis less bent on

visibility/invisibility binaries could tease out some new ways of thinking through autonomy, power, control, and the body.

Resistance and Refusal: A Purview

If surveillance is absolute and privacy is obsolete, then is resistance even an option? Could we imagine a border, for example, without automated security? Would Microsoft's Tay.AI have lived a longer digital life if the chatbot wasn't gendered? And what if race and gender as a technology weren't baked into digital mediation, including in the deepfakes that have become the collective internet's shiny new ball, subsequently catching the eye of a myriad of security apparati around the globe? Of course, attempting to answer these questions is a Sisyphean task because the frameworks, assemblages and technologies replicating discrimination, Othering and exclusionary tactics do not operate independently, but collectively — together. They are like a tangled ball of string — or perhaps more apropos for this study, a tangled mass of computer wires. Each wire leads somewhere, each does something. But disentangling the wires is near impossible if not completely so. And not just that: the wires are duplicative — replicating their features and objectives across the system as a whole, again and again and again. Despite the daunting nature of the work, Bauman and Lyon (2013) posit, there is reason for hope because there is agency — and humanity. "Hope nowadays feels frail, vulnerable, fissiparous precisely because we can't locate a viable and sufficiently potent agency that can be relied on to make the words flesh," Bauman says, in his conversation with Lyon (2013, 147. He continues:

> We hope for hope — for a better grounded, more hopeful hope …
> In the digital facility to summon thousands of men and women to a

> public square we try hard to spy out a promise of construction a new regime that will put paid to the oddities and inanities of the present one. This is OK, and for our mental sanity most welcome, as long as we go on hoping; it is much less helpful when we proclaim (or accept other's proclamations) that the case that such a regime will fulfill it successfully has already been opened and closed (2013, 187).

In other words, we must retain our critical gaze. And while it is often the more entertaining, easier to handle, and generally more pleasant option, we cannot allow the siren call of the blob's all-encompassing environment to completely take us over. One such valuable critical exercise happens when considering normative/non-normative counter-surveillance tactics in the hopes of approaching them with an eye for both their underlying theoretical assumptions and what they offer in terms of freedom and subject agency against the very real consequences of state surveillance and control. A central task of this academic project is unpacking the ways we can conceptualize identity via an aesthetics of counter-surveillance and visibility. One modern work of art helps tell exactly that story, providing in the form of creative critique. It's called Facial Weaponization: Fag Face Mask. The project's central component resembles, in color and shape (or, shapelessness) a wad of chewed bubble gum on top of a human torso (Blas & Gaboury 2016) . A blob within a blob to critique, perhaps, a blob.

Part of a larger art project by Zach Blas that seeks to make visible the "practices of surveillance that both identify individual subjects and generalize broad populations," the mask is designed from the aggregated biometric data of many queer men's faces. Fag Face Mask, as it's designed, is meant to suggest that queer politics don't necessarily cohere to biometric standardization — when you aggregate faces, but don't average them, you're left with the excess that these faces produce together. Fag Face Mask is indicative of a form of informatic opacity, or opacity as an uncategorizable alterity that defies standardization.

Similarly, the masks of Facial Weaponization Suite are designed to be both objects of visibility and invisibility, an inversion of both the social impetus towards a visible face, and the counter-surveillance tactic of obfuscation. Aligning his work with the masks used by The Zapatista Army, Anonymous, Pussy Riot, and Black Bloc, Blas argues that he hides the face so that it's seen; that facelessness is a political transformation into something unknown and unidentified. And, as well, Blas critiques both privacy and transparency. Of the former, he shares Bratton's hesitation at the potentialities of neoliberal immunization from collective accountability (Blas & Gaboury 2016). Of the latter, he channels Edouard Glissant in labelling transparency as barbaric and bound to a kind of Western universalism. Interesting here is the interplay of sight and universalisms — alterity is both visible within systems of standardization and invisible; the reason for both being because it can't be standardized. This weird sight/non-sight imbued within Fag Face Mask gets past the notion of the face as an identifier; it escapes that faciality of reference that Guattari talks about in The Machinic Unconscious (2010).

One might argue the more interesting aspect of Fag Face Mask is not, necessarily, the opacity it cultivates in the same oeuvre as anonymizing radical activism, but rather in the way it mirrors our own identities back to us as a reverse "uncanny valley" (2012). Where Masahiro Mori's original valley describes the creepiness of how slightly inhuman a thing appears, the reverse explains our revulsion at how un-human we begin to appear as we look at ourselves through the thing's eyes. Blas' masks, a reworking of the same data collection methodologies used for the surveillance and capture of aggregate faces, presents an uncomfortable insight into the subject as seen via big data standardization and control mechanisms, and at the same time, a methodological and ethical quandary. What does it mean to use surveillance technologies and data aggregation methods as a mode of counter-surveillance and opacity? Does Blas' mask

present a true counter to the alterity-deleting and dangerous-face highlighting of facial recognition and expression tracking, or does it reproduce a violence similar to the one it purports to confront?

Put another way, are the problems of surveillance inherent to the programmatic logics of data collection? While Blas argues that in his work the face is a norm of interpretation and that "the materiality of the head can never be reduced to the face, which is purely signification," (Blas & Gaboury 2016) this does suggest that countersurveillance techniques and strategies need to be cognizant of the problematics of approaching surveillance and privacy through an Orwellian paranoid-dystopian binary.

Seda Gurses, Arun Kundnani, and Joris Van Hoboken take up a similar question in their work on counter-surveillance advocacy (2016). Critiquing the discourse and economic assimilation of encryption or "crypto" technologies against targeted surveillance, they argue any counter to surveillance should look outside the realm of the techno and legal field and focus on what surveillance is used for: The maintenance of a neoliberal empire structured by racial, gender, and economic inequalities. In the art installation Street with a View, Ben Kinsley and Robin Hewlitt (2008) also poke at the invisible/visible binary. For the pieces, residents of Pittsburgh's Northside were asked to stage a number of scenes — a parade, a marathon, a heroic rescue, a sword fight — as Google's Street View team drove through their neighborhood. The images, uploaded to Google Maps, present a different sort of playful "masking" against spatialized surveillance, one dependent on the performative. Similar to Blas' work, Street with a View contends that the interpolation between visibility and invisibility, between surveillance and opacity, doesn't have to be a clearcut distinction.

Instead, participants knowingly engaged in a performative re-working of the technologies meant to record their experiences by adding in a touch of the ridiculous and out-of-place. These aesthetic responses to surveillance don't mitigate the dangers posed to vulnerable populations, but they do provide a different way of approaching it — one more cognizant that privacy itself is political and that it resides in networks of race, gender, sex, and othering that limits the activism it inspires.

Works Cited

Agamben, Giorgio. *Homo Sacer: Sovereign Power and Bare Life* Stanford: Stanford University Press, 1998.

Alba, Davey. "It's Your Fault Microsoft's Teen Ai Turned into Such a Jerk." *Wired*, March 25, 2016. http://www.wired.com/2016/03/fault-microsofts-teen-ai-turned-jerk.

Althusser, Louis, Etienne Balibar, Jacques Bidet, and G. M. Goshgarian. *On the reproduction of capitalism: Ideology and ideological state apparatuses.* London: Verso, 2014.

Amar, Paul. *The Security Archipelago: Human-Security States, Sexuality Politics, and the End of Neoliberalism.* Durham: Duke University Press Books, 2013.

Amnesty International. "Troll Patrol Findings: Using Crowdsourcing, Data Science, and Machine Learning to Measure Violence and Abuse against Women on Twitter." Troll Patrol Report. Accessed November 20, 2022. https://decoders.amnesty.org/projects/troll-patrol/findings.

Amoore, Louise, and Alexandra Hall. "Taking People Apart: Digitised Dissection and the Body at the Border." Environment and Planning: Society and Space 27, no. 3 (2009): 444–64. https://doi.org/10.1068/d1208.

Amoore, Louise. *The Politics of Possibility Risk and Security Beyond Probability.* Durham: Duke University Press, 2013.

Andrejevic, M. in Dubrofsky, "Foreword." In *Feminist Surveillance Studies*. ix-xviii. Rachel E., and Shoshana Amielle Magnet, eds. Duke University Press, 2015.

Anti-Defamation League. n.d. "Alt Right: A Primer on the New White Supremacy." Accessed January 7, 2022. https://www.adl.org/resources/backgrounders/alt-right-a-primer-about-the-new-white-supremacy.

Aradau, Claudia, and Jef Huysmans. "Critical Methods in International Relations: The Politics of Techniques, Devices and Acts." European Journal of International Relations 20, no. 3 (2013): 596–619. https://doi.org/10.1177/1354066112474479.

Baig, Edward C. "IPhone X First Look: Face ID Passes Our Quick Tests and 'animojis' Are Addictive." USA Today, October 31, 2017. https://www.usatoday.com/story/tech/columnist/baig/2017/10/31/iphone-x-first-look-face-id-passes-our-quick-tests-and-animojis-addictive/815985001/.

Balsamo, Anne. 1996. Technologies of the Gendered Body: Reading Cyborg Women. Durham, NC: Duke University Press.

Banet-Weiser, Sarah. Empowered: Popular Feminism and Popular Misogyny. Durham: Duke University Press Books, 2018.

Beauchamp, Zack. 2018. "Unite the Right 2018: 11 Million White Americans Think like Alt-Righters." Vox, August 10. https://www.vox.com/2018/8/10/17670992/study-white-americans-alt-right-racism-white-nationalists.

Bernays, Edward. “The Engineering of Consent.” The ANNALS of the American Academy of Political and Social Science. 250, no. 1 (March 1947).

Bernays, Edward. “Manipulating Public Opinion: The Why and The How.” American Journal of Sociology. 33, no. 6 (May 1928).

Bernstein, Basil. *Class, Codes, and Control. Volume 3: Towards a Theory of Educational Transmissions.* London: Routledge & Kegan Paul, 1975.

Bertillion, A. *Tableau synoptic des traits physionomiques.* Metropolitan Museum of Art, New York, 1909.

Biscobing, D. “Too Far? Future of lie detection being written in Arizona.” ABC15 Arizona, 2013. https://www.youtube.com/watch?v=QuFvNiBosM8

Blas, Zach and Gaboury, Jacob. “Biometrics and Opacity: A Conversation.” Camera Obscura 31, no. 2 (2016): 155-165.

Bollen, Y. “The Future of Mass Surveillance Is Here (and We Are Excited about It).” Masters of Media, December 22, 2022. https://mastersofmedia.hum.uva.nl/blog/2017/09/24/the-future-of-mass-surveillance-is-here-and-we-are-excited-about-it/.

Bourne, Mike, Heather Johnson, and Debbie Lisle. “Laboratizing the Border: The Production, Translation and Anticipation of Security Technologies.” Security Dialogue 46, no. 4 (2015): 307–25. https://doi.org/10.1177/0967010615578399.

Bowles, Nellie. 2016. “‘She Has a Name’: Amazon’s Alexa Is a Sleeper Hit, with Serious Superfans.” The Guardian, April 26. https://www.theguardian.com/technology/2016/apr/26/amazon-echo-alexa-voice-recognition-superfans.

Bratton, Benjamin H. *The Stack: On Software and Sovereignty.* Massachusetts: MIT Press, 2016.

Bright, Peter. 2016. “Tay, the Neo-Nazi Millennial Chatbot, Gets Autopsied.” Ars Technica, March 25. http://arstechnica.com/information-technology/2016/03/tay-the-neo-nazi-millennial-chatbot-gets-autopsied

Bousquet. *The Eye of War: Military Perception from the Telescope to the Drone.* University of Minnesota Press, 2018.

Britt Paris, and Joan Donovan. “Deepfakes and Cheap Fakes: The Manipulation of Audio and Visual Evidence.” Media Manipulation. Data & Society, September 2019. https://datasociety.net/library/deepfakes-and-cheap-fakes/.

Brocklehurst, H., 2021. Where is the “am I the drama” sound from that’s all over TikTok rn? [WWW Document]. UK. URL https://thetab.com/uk/2021/06/28/am-i-the-drama-sound-tiktok-212391 (accessed 6.14.23).

Broeders, Dennis, and Huub Dijstelbloem. “The Datafication of Mobility and Migration Management.” In *Digitizing Identities: Doing Identity in a Networked World*, Irma Van De Ploeg and Jason Pridmore, eds. Routledge, 2015, https://doi.org/10.4324/9781315756400-13.

Browne, Simone. *Dark Matters: On the Surveillance of Blackness.* Durham: Duke University Press Books, 2015.

Bumiller, Kristin. *In an Abusive State: How Neoliberalism Appropriated the Feminist Movement Against Sexual Violence*. Illustrated edition. Durham: Duke University Press Books, 2008.

Burgess, Matt. "Deepfake Porn Is Now Mainstream. And Major Sites Are Cashing In." *Wired UK*. Accessed January 25, 2022. https://www.wired.co.uk/article/deepfake-porn-websites-videos- law.

Burgess, Matt. "The Biggest Deepfake Abuse Site Is Growing in Disturbing Ways." *Wired.* Accessed January 25, 2022. https://www.wired.com/story/deepfake-nude-abuse/.

Butler, J. *Bodies That Matter: On the Discursive Limits of Sex*, Hoboken: Routledge, 2011.

Carter, S.K., Paul Lushenko, and Keith, 2023. Lessons from the meme war in Ukraine. Brookings. https://www.brookings.edu/techstream/lessons-from-the-meme-war-in-ukraine/ (accessed 6.14.23).

Carrie. 1976. Directed by Brian de Palma. Los Angeles: United Artists.

Chang, Lulu. 2016. "Microsoft's Cortana Gets Sexually Harassed, but She Fights Back." *Digital Trends*, February 7. https://www.digitaltrends.com/cool-tech/microsoft-cortana-sexual-harassment/.

Chayka, Kyle., 2022. "Ukraine Becomes the World's 'First TikTok War'" *The New Yorker*. https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war.

Chesney, Robert, and Danielle K. Citron. "Disinformation on Steroids: The Threat of Deep Fakes." *Council on Foreign Relations*. Accessed January 25, 2022. https://www.cfr.org/report/deep-fake-disinformation-steroids.

Chiel, Ethan. 2016. "Who Turned Microsoft's Chat Bot Racist? Surprise, It Was 4chan and 8chan." *Splinter*, March 24. https://splinternews.com/who-turned-microsofts-chatbot-racist-surprise-it-was-1793855848.

Chun, Wendy Hui Kyong. *Programmed Visions: Software and Memory*. MIT Press, 2011.

Chun, Wendy Hui Kyong. 2011b. Programmed Visions: Software and Memory. Cambridge, MA: MIT Press. ———. 2011b. "Race and/as Technology, or How to Do Things with Race." In Race after the Internet, edited by Lisa Nakamura and Peter A. Chow-White, 38–60. New York: Routledge.

Chun, Wendy Hui Kyong. "Race and/as Technology, or How to Do Things with Race." In *Race After the Internet*, edited by Lisa Nakamura and Peter Chow-White, 38–60. New York: Routledge, 2011.

Cole, Samantha. "There Is No Tech Solution to Deepfakes." *Vice* (blog), August 14, 2018. https://www.vice.com/en/article/594qx5/there-is-no-tech-solution-to-deepfakes.

Coleman, Beth. 2009. "Race as Technology." *Camera Obscura* 24(1):177–207.

Creed, Barbara. 1986. “Horror and the Monstrous Feminine: An Imaginary Abjection.” *Screen* 27(1):44–71. 1994. The Monstrous Feminine: Film, Feminism, Psychoanalysis. New York: Routledge.

Collis, Avinash, Alex Moehring, Sen Ananya, Alessandro Acquisti. “Quantifying the user value of social media data.” Penn Carey Law, University of Pennsylvania. https://www.law.upenn.edu/live/blogs/78-quantifying-the-user-value-of-social-media-data#:~:text=We%20found%20that%20the%20median,settlements%20and%20Facebook's%20revenue%20projections, November 1, 2001.

Cooper-Cunningham, Dean. “Security, Sexuality, and the Gay Clown Putin Meme: Queer Theory and International Responses to Russian Political Homophobia.” *Security Dialogue* 53, no. 4 (2022): 302–23. https://doi.org/10.1177/09670106211055308.

Craggs, Ryan. “Dubai’s Latest Airport Security Innovation? Face-Scanning Virtual Aquariums.” *Condé Nast Traveler*, October 11, 2017. https://www.cntraveler.com/story/dubai-international-airport-is-installing-face-scanning-aquariums.

Crary, Jonathan. *Suspensions of Perception: Attention, Spectacle, and Modern Culture.* Cambridge, Massachusetts: MIT Press, 2001.

Dagognet, François. *Faces, surfaces, Interfaces.* Librarie Philosophique J. Paris: Vrin, 1982.

Daly, Mary. 1990. Gyn/Ecology: The Metaethics of Radical Feminism. Boston: Beacon. Daniels, Jessie. 2013. “Race and Racism in Internet Studies: A Review and Critique.” *New Media and Society* 15(5):695–719.

Dang, S., Culliford, E., 2022. TikTok war: How Russia’s invasion of Ukraine played to social media’s youngest audience. Reuters. https://www.reuters.com/technology/tiktok-war-how-russias-invasion-ukraine-played-social-medias-youngest-audience-2022-03-01 (accessed 6.14.23).

de Lauretis, Teresa. 1987. *Technologies of Gender: Essays on Theory, Film, and Fiction*. Bloomington: Indiana University Press.

Delgado, Richard, and Jean Stefancic. 2001. *Critical Race Theory: An Introduction.* New York: New York University Press.

Deleuze, G., Guattari, F. *A Thousand Plateaus: Capitalism and Schizophrenia*, University of Minnesota Press, Minneapolis, 1987

Deleuze, G. (translated by Paul Patton). *Difference and Repetition.* Columbia University Press. New York, 1995.

DePaulo, B.M, Lindsay, J.J., Malone, B.E., Muhlenbruck, L., Charlton, K., Cooper, H. (2003). Cues to Deception. *Psychological Bulletin* 129, pp. 74–118.

DiNucci, Darcy. 1999. “Fragmented Future.” *Print* 53(4):32, 221–22.

Dubrofsky, Rachel E., and Shoshana Amielle Magnet, eds. *Feminist Surveillance Studies*. Durham: Duke University Press Books, 2015.

Duchenne, Guillaume-Benjamin, and R. Andrew Cuthbertson. *The Mechanism of Human Facial Expression.* Cambridge: University Press, 2006.

Dyson, George. *Darwin among the Machines: The Evolution of Global Intelligence.* New York: Basic Books, 2012.

Eastwood, S.C., Shmerko, V.P., Yanushkevich, S.N., Drahansky, M. (2014). *Biometric Intelligence in Authentication Machines: From Talking Faces to Talking Robots*. Presented at the IIAI 3rd International Conference on Advanced Applied Informatics, pp. 763–768.

Edkins, J., V. Pin-Fat, Shapiro, M. J., (2004). *Sovereign Lives. Power in Global Politics.* Routledge: London.

Edkins, J. (2015). *Face Politics.* Routledge, London ; New York.

Elgan, Mike. 2018. "Why Google Assistant Will Beat Siri, Alexa, and Cortana." Computerworld, May 5. https://www.computerworld.com/article/3269753/digital-assistants/why-google-assistant-will-beat-siri-alexa-and-cortana.html. Ex Machina. 2014. Directed by Alex Garland. London: DNA Films.

Ekman, P., (2007). *Emotions Revealed, Second Edition: Recognizing Faces and Feelings to Improve Communication and Emotional Life*, 2nd edition. ed. Holt Paperbacks, New York.

Ekman, P., (1999). Basic Emotions, in: Dalgleish, T., Power, M. (Eds.), *Handbook of Cognition and Emotion.* John Wiley & Sons Ltd., University of California, San Francisco, CA USA, pp. 44 - 60.

Ekman, P., Friesen, W.V. (1980). Facial Signs of Emotional Experience. *Journal of Personality and Social Psychology* 39, pp. 1123–1134.

Ekman, P., Friesen, W.V. (1971). Constants Across Cultures in the Face and Emotion. *Journal of Personality and Social Psychology* 17, pp. 123–129.

Ekman, P., Friesen, W. V. (1969). Nonverbal Leakage and Clues to Deception. *Psychiatry* 32, pp. 88–106.

Epstein, C. (2008.) "Embodying Risk: Using Biometrics to Protect the Borders." In *Risk and the War on Terror*, edited by Louise Amoore and Marieke de Goede. New York, NY: Routledge.

Epstein, C. (2016). Surveillance, Privacy and the Making of the Modern Subject: Habeas what kind of Corpus? *Body & Society*, 22(2), 28-57. https://doi.org/10.1177/1357034X15625339

Fassin, Didier. *Enforcing Order: An Ethnography of Urban Policing.* New York: Polity, 2013.

Fessler, Leah. "We Tested Bots like Siri and Alexa to See Who Would Stand up to Sexual Harassment." *Quartz*, February 22, 2017. https://qz.com/911681/we-tested-apples-siri-amazon-echos-alexa-microsofts-cortana-and-googles-google-home-to-see-which-personal-assistant-bots-stand-up-for-themselves-in-the-face-of-sexual-harassment.

Foer, Franklin. "The Era of Fake Video Begins." *The Atlantic*, April 8, 2018. https://www.theatlantic.com/magazine/archive/2018/05/realitys-end/556877/.

Foucault, Michel, (1982). The Subject and Power. *Critical Inquiry* 8(4), pp. 777– 795.

Foucault, Michel. (1995) *Discipline and Punish: The Birth of the Prison*. Vintage Books, New York, 215.

Foucault, Michel. *The History of Sexuality, Vol. 1: An Introduction*. Translated by Robert Hurley. Reissue edition. New York: Vintage, 1990.

Franks, Mary Anne in Renée Heberle. 2006. *Feminist Interpretations of Theodore Adorno: Re-reading the Canon.* University Park: Penn State Press.

Freedman, Carl. (2000). *Critical Theory and Science Fiction*. Middletown, CT: Wesleyan University Press.

FRONTEX (2016). Best Practice Operational Guidelines for Automated Border Control (ABC) Systems. Available at: https://publications.europa.eu/en/publication-detail/-/publication/e81d082d-20a8-11e6-86d0-01aa75ed71a1/language-en (accessed 10.30.18)

Fuller, M. & Goffey, A. *Evil Media*. Cambridge, Massachuetts: MIT Press, 2012.

Fung, Brian. 2016. "Why Microsoft's Racist Twitter Bot Should Make Us Fear Human Nature, Not A.I." Washington Post, March 24. https://www.washington post.com/news/the-switch/wp/2016/03/24/why-microsofts-racist-twitter-bot -should-make-us-fear-human-nature-not-a-i/?noredirect5on.

Gallagher, R., Jona, L. (2019). We Tested Europe's New Lie Detector for Travelers — And Immediately Triggered a False Positive. *The Intercept.* Available at: https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/

Galloway, A.R., (2012). *The Interface Effect*, 1 edition. ed. Polity, Cambridge, UK ; Malden, MA.

Galton, F., (1883). *Inquiries into Human Faculty.* London: The Eugenics Society

Gates, K.A. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. NYU Press, New York.

Goldberg, D.T. (2002). *The Racial State*. Blackwell Publishers. NY, New York.

Gordin, Colin. "Governmental Rationality: An Introduction," in The Foucault Effect: Studies in Governmentality, ed. Graham Burchell, Colin Gordon, and Peter Miller (Chicago: University of Chicago Press, 1991). 1-52

Gosse, Chandell, and Jacquelyn Burkell. "Politics and Porn: How News Media Characterizes Problems Presented by Deepfakes." Critical Studies in Media Communication 37, no. 5 (October 19, 2020): 497–511. https://doi.org/10.1080/15295036.2020.1832697.

Grewal, Inderpal. *Saving the Security State: Exceptional Citizens in Twenty-First-Century America.* Durham: Duke University Press Books, 2017.

Guattari, F. (2010). *The Machinic Unconscious: Essays in Schizoanalysis*. Semiotext, Los Angeles, CA : Cambridge, Mass.

Guerrero, Lisa. "Can I Live? Contemporary Black Satire and the State of Postmodern Double Consciousness." Studies in American Humor 2, no. 2 (2016): 266–79. https://doi.org/10.5325/studamerhumor.2.2.0266.

Gustavsson, Eva. 2005. "Virtual Servants: Stereotyping Female Front-Office Em- ployees on the Internet." Gender, Work, and Organization 12(5):400–419. Hall, Stuart. 1997. "The Spectacle of the 'Other.'" In *Representation: Cultural Representations and Signifying Practices*, 223–79. London: Sage.

Gurses, Seda, Kundnani, Arun & Hoboken, Joris Van. "Crypto and empire: the contradictions of counter-surveillance advocacy," *Media, Culture & Society* 38, no. 4 (2016). https://doi.org/10.1177/0163443716643006

Hall, R. (2015). *The Transparent Traveler: The Performance and Culture of Airport Security*. Duke University Press Books, Durham.

Hall, A. (2017). Decisions at the Data Border: Discretion, Discernment, and Security. *Security Dialogue* 48, 488–504.

Halpern, Orit. *Beautiful Data: A History of Vision and Reason Since 1945*. London: Duke University Press, 2014.

Haraway, Donna. 1990. *Simians, Cyborgs, and Women: The Reinvention of Nature.* New York: Routledge.

Haraway, Donna. 2006. A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late 20th Century. In: Weiss, J., Nolan, J., Hunsinger, J., Trifonas, P. (eds) *The International Handbook of Virtual Learning Environments*. Springer, Dordrecht. https://doi.org/10.1007/978-1-4020-3803-7_4

Hay, Zachary. "Towards Trans-Inclusive AI," *Medium*, Towards Data Science. May 13, 2019, https://towardsdatascience.com/towards-trans-inclusive-ai-a4abe9ad4e62.

Hayles, Katherine N. (1999). *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*, University Of Chicago Press, Chicago, Ill.

Her. 2013. Directed by Spike Jonze. Los Angeles: Annapurna Pictures.

Hester, Helen. 2016. "Technically Female: Women, Machines, and Hyper-employment." Salvage, August 8. http://salvage.zone/in-print/technically-female-women-machines-and-hyperemployment.

Hill, Jennifer, Randolph Ford, and Ingrid G. Farreras. 2015. "Real Conversations with Artificial Intelligence: A Comparison between Human–Human Online Conversations and Human–Chatbot Conversations." Computers in Human Behavior 49:245–50.

Hobbes, *The Leviathan*, ed. C.B. MacPherson. (New York: Penguin Group, 1982).

Hochschild, Arlie Russell. 1983. *The Managed Heart: The Commercialization of Human Feeling.* Berkeley: University of California Press.

Holmes, Janet. 1995. *Women, Men, and Politeness.* London: Longman.

iMotions (n.d.)Biometric Research, Simplified. iMotions. Available at: https://imotions.com/ (accessed 10.26.18).

Jenkins, Henry. 2002. "Cyberspace and Race." MIT Technology Review, April 1. https://www.technologyreview.com/2002/04/01/101999/cyberspace-and-race/. Jennifer's Body. 2009. Directed by Karyn Kusama. Century City, CA: Twentieth-Century Fox.

Kanai, Akane. 2017. "On Not Taking the Self Seriously: Resilience, Relatability, and Humour in Young Women's Tumblr Blogs." *European Journal of Cultural Studies* 22(1):60–77.

Kantar Added Value (n.d.). What do Women Want? Available at: http://added-value.com/casestudy/diageo-3/ (accessed 10.26.18)

Kantrowitz, Alex. 2016. "Microsoft's New AI-Powered Chatbot Mimics a 19-Year-Old American Girl." BuzzFeed News, March 23. https://www.buzzfeednews.com/article/alexkantrowitz/microsoft-introduces-tay-an-ai-powered-chatbot-it-hopes-will

Keene, Jamie. 2012. "Steve Jobs Didn't Like Siri's Name, Couldn't Think of Anything Better." The Verge, March 28. https://www.theverge.com/2012/3/28/2908658/steve-jobs-unconvinced-name-siri.

Kendall, Lori. 2002. *Hanging Out in the Virtual Pub: Masculinities and Relationships Online*. Berkeley: University of California Press.

Kinsley, Ben & Robin Hewlitt. "Street with a View." Art Installation (2008). https://benkinsley.com/street-with-a-view/

Kleeman, Sophie. 2016. "Here Are the Microsoft Twitter Bot's Craziest Racist Rants." *Gizmodo*, March 24. https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160.

Kristeva, Julia. 1982. *Powers of Horror: An Essay on Abjection*. Translated by Leon Roudiez. New York: Columbia University Press.

Lane, Keiko in Taormino, Tristan, Celine Parrenas Shimizu, Constance Penley and Mireille Miller-Young. 2013. *The Feminist Porn Book: The Politics of Producing Pleasure*. The Feminist Press: New York.

Latour, Bruno. *Science in Action: How to Follow Scientists and Engineers Through Society*. Revised ed. edition. Cambridge, Mass: Harvard University Press, 1988.

Lavater, Johann, C. (1840) *Essays on Physiognomy*. London: Thomas Tegg.

Lee, Peter. 2016. "Learning from Tay's Introduction." Official Microsoft Blog, March 25. https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/.

"Lie-Detecting Kiosks Are Coming to an Airport near You." Yahoo! News. Accessed November 20, 2023. https://www.yahoo.com/news/lie-detecting-kiosks-coming-airport-near-001642958.html.

Lyon, David. (2002) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. Routledge

Mack, D., 2018. This PSA About Fake News From Barack Obama Is Not What It Appears BuzzFeed News. https://www.buzzfeednews.com/article/davidmack/obama-fake-news-jordan-peele-psa-video-buzzfeed

MacLeod, V., McLindin, B. (2011). Methodology for the Evaluation of an International Airport Automated Border Control Processing System, in: Jain, L.C., Aidman, E.V., Abeynayake, C. (Eds.), *Innovations in Defence Support Systems -2: Socio-Technical Systems, Studies in Computational Intelligence.* Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 115–145.

Maddocks, Sophie. "'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities between Pornographic and 'Political' Deep Fakes." Porn Studies 7, no. 4 (October 1, 2020): 415–23. https://doi.org/10.1080/23268743.2020.1757499.

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

Marino, Mark C. 2014. "The Racial Formation of Chatbots." CLCWeb: Comparative Literature and Culture 16(5). https://docs.lib.purdue.edu/clcweb/vol16/iss5/13/.

Markoff, John, and Paul Mozur. 2015. "For Sympathetic Ear, More Chinese Turn to Smartphone Program." New York Times, August 4. https://www.nytimes.com/2015/08/04/science/for-sympathetic-ear-more-chinese-turn-to-smartphone-program.html.

Massanari, Adrienne. 2017. "#Gamergate and the Fappening: How Reddit's Algo- rithm, Governance, and Culture Support Toxic Technocultures." *New Media and Society* 19(3):329–46.

Massumi, Brian. "Fear (The Spectrum Said)." *positions: east asia cultures critique*, Duke University Press. 13, no. 1 (2005): 31-48.

Matsumoto, D,, et al. (2014) Reading People: Behavioral Anomalies and Investigative Interviewing, March 4. FBI: Law Enforcement Bulletin. Available at: https://leb.fbi.gov/articles/featured-articles/reading-people-behavioral-anomalies-and-investigative-interviewing (accessed 8.26.18).

Metropolis. 1927. Directed by Fritz Lang. Brandenburg: UFA.

Metz, Rachel. 2018. "Microsoft's Neo-Nazi Sexbot was a Great Lesson for Makers of AI Assistants." MIT Technology Review, March 28. https://www.technologyreview.com/s/610634/microsofts-neo-nazi-sexbot-was-a-great-lesson-for-makers-of-ai-assistants/.

Mirovalev, M., n.d. As bombs fall on Ukraine, memes ridicule Russian aggression [WWW Document]. URL https://www.aljazeera.com/news/2022/3/10/ukrainian-wartime-humour-derides-and-ridicules-russia.

Mori, M. (2012). Translated by MacDorman, K. F.; Kageki, Norri. The Uncanny Valley. *IEEE Robotics and Automation*. 19 (2): pp. 98–100.

Morais, Betsy. 2013. "Can Humans Fall in Love with Bots?" New Yorker, November 19. https://www.newyorker.com/tech/annals-of-technology/can-humans-fall-in-love-with-bots.

Muller, Benjamin J. *Security, Risk and the Biometric State: Governing Borders and Bodies*. 1 edition. London: New York: Routledge, 2010

Muller, B.J. (2015). AVATAR, in: *Making Things International 1*. University of Minnesota Press, Minneapolis, MN, pp. 49–61.

Nakamura, Lisa. 2002. Cybertypes: Race, Ethnicity, and Identity on the Internet. New York: Routledge. ———. 2007. Digitizing Race: Visual Cultures of the Internet. Minneapolis: University of Minnesota Press.

Nagle, Angela. 2017. Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the Alt-Right. Winchester: Zero.

Nakamura, Lisa, Hanah Stiverson, and Kyle Lindsey. *Racist Zoombombing*. 1st edition. Routledge, 2021.

National Security Challenges of Artificial Intelligence, Manipulated Media, and 'Deepfakes': Permanent Select Committee on Intelligence (2019). https://www.congress.gov/event/116th-congress/house-event/109620.

Neff, Gina, and Peter Nagy. 2016. "Talking to Bots: Symbiotic Agency and the Case of Tay." *International Journal of Communication* 10:4915–31.

Nelson, Alondra. *Race After the Internet*. Edited by Lisa Nakamura and Peter Chow-White. New York: Routledge, 2011.

Newton, Casey. 2018. "Twitter Will Hide More Bad Tweets in Conversations and Searches." The Verge, May 15. https://www.theverge.com/2018/5/15/17352962/twitter-abuse-changes-ranking-tweets-conversations-search.

Nunamaker, J.F., Derrick, D.C., Elkins, A.C., Burgoon, J.K., Patton, M.W. (2011). Embodied Conversational Agent-Based Kiosk for Automated Interviewing. *Journal of Management Information Systems* 28 (1), pp. 17– 48.

Ohman, Richard. *Selling Culture: Magazines, Markets and Class at the Turn of the Century*. London: Verso, 1998.

O'Reilly, Tim. 2005. "What Is Web 2.0." O'Reilly Network, September 30. https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html.

Parker, N. and Vaughan-Williams N. (2012). Critical Border Studies: Broadening and Deepening the 'Lines in the Sand" Agenda. *Geopolitics* 17 (4). 727 – 733.

Pateman, Carole. 1988. The Sexual Contract. Cambridge: Polity.

Penley, Constance in Taormino, Tristan, Celine Parrenas Shimizu, Constance Penley and Mireille Miller-Young. 2013. *The Feminist Porn Book: The Politics of Producing Pleasure.* The Feminist Press: New York.

Pentland, S., Twyman, N, Burgoon, J., Nunamaker J., Diller, C., (2017). A Video-Based Screening System for Automated Risk Assessment Using Nuanced Facial Features, *Journal of Management Information Systems*, 34:4, pp. 970-993.

Pepi, n.d. Benjamin Bratton | Machine Vision. DIS Magazine. http://dismagazine.com/discussion/73272/benjamin-bratton-machine-vision/

Phillips, Whitney. *This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture*. Cambridge, Massachusetts: MIT Press, 2015

Puar, Jasbir K. *Terrorist Assemblages: Homonationalism in Queer Times*. Durham: Duke University Press Books, 2017.

Power, Nina. 2017. "Soft Coercion, the City, and the Recorded Female Voice." December 7. https://ninapower.net/2017/12/07/soft-coercion-the-city-and-the-recorded-female-voice/.

Protobrand (n.d.) Market Research. Available at: http://www.protobrand.com (accessed 10.26.18).

Pugliese, J., (2005). "In Silico Race and the Heteronomy of Biometric Proxies: Biometrics in the Context of Civilian Life, Border Security, and Counter-Terrorism Laws." *Australian Feminist Law Journal* 23. Pp. 1 – 32.

Pugliese, Joseph. *Biometrics: Bodies, Technologies, Biopolitics*. 1 edition. New York: Routledge, 2010.

Qualtrics (n.d.) The Leading Research & Experience Software Available at: https://www.qualtrics.com/ (accessed 10.26.18).

Rinelli, Alysso. "Unraveling The Legal Landscape Of Deepfake Porn." *Evie Magazine,* August 2023. https://www.eviemagazine.com/post/unraveling-the-legal-landscape-of-deepfake-porn-protecting-women-gaps

Romano, Aja. "Jordan Peele's Simulated Obama PSA Is a Double-Edged Warning against Fake News." Vox, April 18, 2018. https://www.vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed.

Salter, M.B. (2007a). Governmentalities of an Airport: Heterotopia and Confession. *International Political Sociology* 1, pp. 49–66.

Salter, M.B. (2007b). We are all exiles: implications of the border as a state of exception, in: *Contemporary Insecurities and the Politics of Exception*. Presented at the Standing Group on International Relations Conference, Turin, Italy.

Salter, Michael. 2017. Crime, Justice, and Social Media. London: Routledge. ———. 2018. "Publicising Privacy, Weaponising Publicity: The Dialectic of Online Abuse on Social Media." In Digital Intimate Publics and Social Media, edited by Amy Shields Dobson, Brady Robards, and Nicholas Carah, 29–43. Cham: Pal- grave Macmillan.

Salter, M.B. (2012). Theory of the Suture and Critical Border Studies. *Geopolitics* 17 (4): pp. 734 – 735

Schlag, P. (1997). Commentary: Law and Phrenology. *Harvard Law Review* 97, pp. 1 – 39.

Schottmiller, Carl. (2017). *Reading RuPaul's Drag Race: Queer Memory, Camp Capitalism, and RuPaul's Drag Empire.* Dissertation: University of California, Los Angeles.

Senechal, T., Turcot, J., Kaliouby, R.E. (2013). Smile or Smirk? Automatic Detection of Spontaneous Asymmetric Smiles to Understand Viewer Experience. *Face & Gesture Conference.*

Sensity. "Mapping the Deepfake Landscape." Medium, November 29, 2019. https://medium.com/sensity/mapping-the-deepfake-landscape-27cb809e98bc.

Shaviro, Steven. 2003. *Connected, or What It Means to Live in the Network Society*. Minneapolis: University of Minnesota Press.

Shaviro, Steven, 2016. *Discognition.* New York: Repeater Books.

Slootmaeckers, Koen. "Nationalism as Competing Masculinities: Homophobia as a Technology of Othering for Hetero- and Homonationalism." *Theory and Society* 48, no. 2 (2019): 239–65. https://doi.org/10.1007/s11186-019-09346-4.

Simonite, Tom. "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be." Wired. Accessed March 22, 2022. https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook.

Sinders, Caroline. 2016. "Microsoft's Tay Is an Example of Bad Design." Medium, March 24. https://medium.com/@carolinesinders/microsoft-s-tay-is-an-example-of-bad-design-d4e65bb2569f.

Smyth, Dallas. "On the Audience Commodity and its Work." In *Media and Culture Studies,* edited by Meenakshi Durham and Douglas Kellner, 230-256. Oxford: Blackwell Publishing, 1981.

Sosa, Jared. You Won't Believe What Obama Says In This Video!, 2018. https://www.youtube.com/watch?v=cQ54GDm1eL0.

Species. 1995. Directed by Roger Donaldson. Beverly Hills, CA: Metro-Goldwyn- Mayer.

Stiegler, Bernard, *Technics and Time*, trans. Richard Beardsworth and George Collins. Stanford: Stanford University Press, 1998.

Stone, Allucquére Rosanne Sandy. 1991. "Will the Real Body Please Stand Up?: Boundary Stories about Virtual Cultures." In Cyberspace: First Steps, edited by Michael Benedikt, 81–113. Cambridge, MA: MIT Press.

Stuart, Bob. 2014. "#GamerGate: The Misogynist Movement Blighting the Video Games Industry." Daily Telegraph, October 24. https://www.telegraph.co.uk/culture/culturenews/11180510/gamergate-misogynist-felicia-day-zoe-quinn-brianna-wu.html.

Sunden, Jenny. *Material Virtualities: Approaching Online Textual Embodiment*. New edition. New York: Peter Lang Inc., International Academic Publishers, 2003.

The Exorcist. 1973. Directed by William Friedkin. Burbank, CA: Warner Brothers. Fessler, Leah. 2017. "We Tested Bots like Siri and Alexa to See Who Would Stand

Teeth. 2007. Directed by Mitchell Lichtenstein. Los Angeles: Roadside Attractions. Tracy, Liz. 2016. "In Contrast to Tay, Microsoft's Chinese Chatbot, Xiaolce, Is Ac- tually Pleasant." Inverse, March 21. https://www.inverse.com/article/13387-microsoft-chinese-chatbot.

Trim, Craig. 2013. "The Art of Tokenization." Language Processing (blog), January 23. IBM. https://web.archive.org/web/20190530155339/https://www.ibm.com/developerworks/community/blogs/nlp/entry/tokenization?lang5en. Turing, Alan. 1950. "Computing Machinery and Intelligence." Mind 59(236): 433–60.

Tumarkin, P. (2018). UA Licenses Deception-Detecting AVATAR to Startup. UANews. Available at: https://uanews.arizona.edu/story/ua-licenses-deceptiondetecting-avatar-startup (accessed 11.10.18).

Turk, Victoria. "Deepfakes Are Already Breaking Democracy. Just Ask Any Woman." Wired UK. Accessed January 25, 2022. https://www.wired.co.uk/article/deepfakes-pornography.

Twine, R. (2002). Physiognomy, Phrenology, and the Temporality of the Body. *Body & Society*, 8 (1). 67 – 88

Twyman, N.W. (2012). Automated human screening for detecting concealed information. *Department of Management Information Systems*. Tucson, AZ: University of Arizona.

Under the Skin. 2013. Directed by Jonathan Glazer. New York: A24.

Van Dijck, Jose. 2013. The Culture of Connectivity: A Critical History of Social Media. Oxford: Oxford University Press.

Vincent, James. 2016. "Twitter Taught Microsoft's AI Chatbot to Be a Racist Asshole in Less Than a Day." The Verge, March 24. https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist.

Wahl-Jorgensen, Karin, and Matt Carlson. "Conjecturing Fearful Futures: Journalistic Discourses on Deepfakes." Journalism Practice 15, no. 6 (July 3, 2021): 803–20. https://doi.org/10.1080/17512786.2021.1908838.

Wang, Yongdong. 2016. “Your Next New Best Friend Might Be a Robot.” Nautilus, February 4. http://nautil.us/issue/33/attraction/your-next-new-best-friend-might-be-a-robot.

Warwick, Kevin, and Huma Shah. 2015. “Human Misidentification in Turing Tests.” Journal of Experimental and Theoretical Artificial Intelligence 27(2): 123–35.

Watson, Sara. “Data Doppelgängers and the Uncanny Valley of Personalization,” The Atlantic, June 16, 2014. https://www.theatlantic.com/technology/archive/2014/06/data-doppelgangers-and-the-uncanny-valley-of-personalization/372780/

Weil, Simone. (1999). *Formative Writings*. New York, Routledge.

Wiener, Norbert. *Cybernetics: Second Edition: Or the Control and Communication in the Animal and the Machine.* Eastford, Connecticut: Martino Fine Books, 2013.

Wilcox, Lauren. (2015). *Bodies of Violence: Theorizing Embodied Subjects in International Relations*, 1 edition. ed. Oxford University Press, Oxford ; New York.

Wilcox, Lauren. (2017). Embodying Algorithmic War: Gender, Race, and the Posthuman in Drone Warfare. *Security Dialogue* 48, pp. 11–28.

The Witch. 2016. Directed by Robert Eggers. New York: A24.

Wonders, Nancy A. “Global Flows, Semi-Permeable Borders and New Channels of Inequality.” In *Borders, Mobility and Technologies of Control*, edited by Sharon Pickering and Leanne Weber, 63–86. Dordrecht: Springer Netherlands, 2006. https://doi.org/10.1007/1-4020-4899-8_4.

Zevnik, A. (2016). The Politics of the Face: The Scopic Regime and the (un-)masking of the Political Subject. *Journal for Cultural Research* 20, pp. 122–136.