"A Gesture of Defiance" From the Body: Interlocking Consent and The Privacy Aesthetic at the U.S. Southern Border

Charles Woods

Abstract: This essay talks back against using biometrics for bodily control by articulating an intersectional paradigm called "Interlocking Consent" that explains the interlocking nature of various Terms of Service (ToS) policies. Through an analysis of biometrics policies and practices used by the Department of Homeland Security Office of Biometric Identity Management, it amplifies how geo-spatial elements and multiple data usages support privacy erosion and unethical surveillance in the U.S. Southern Border. It posits that understanding how biometrics perpetuate oppression from an intersectional feminist perspective is a critical element of "The Privacy Aesthetic." It defines "The Privacy Aesthetic" as attuning to the oblique ubiquity of rhetorics of privacy and surveillance; recognizing the influence of ToS documents; understanding the intersection of "the body" and "the digital" as essential for new surveillance technologies; and, considering of the importance of space regarding data collection.

Keywords: Data Privacy, Digital Surveillance, Biometrics, Aesthetics, U.S. Southern Border

Doi: https://doi.org/10.37514/PEI-J.2024.27.1.07

This essay was written within the imagined but instituted geographic borders of the state of Texas where I live with my wife and daughter, and where oppressive legislation restricts their bodily autonomy. It is a "gesture of defiance that heals, that makes new life and new growth possible" (hooks 9).

Introduction

The immigrants and asylum seekers who arrive at the United States (U.S.) Southern Border in Texas are not "suspected terrorists, criminals, and immigration violators," as explained by the Office of Biometric Identity Management (OBIM) on the Department of Homeland Security (DHS) website, nor are they committing *migrant crime*, a phrase used by Donald Trump during a 2024 Presidential debate. They are humans seeking the *new life* and *new growth* America has purported to offer, constantly and systematically, since her founding. Unfortunately, privacy erosion abetted by unethical policing via biometrics in this polarizing place shudders those futures and positions *all* immigrants as criminals that must be tracked. "Perhaps we may say," recalling Michel Foucault, "that some of the ideological conflicts that drive today's polemics are enacted between devoted descendants of time and the fierce inhabitants of space" (175).

Charles Woods specializes in digital rhetorics. His scholarship appears in *Computers and Composition, Journal of Interactive Technology and Pedagogy, Peitho, Communication Design Quarterly*, and elsewhere. He is co-editor of The Annual Proceedings of the Computers and Writing Conference. He has received the 2022 & 2024 Kairos John Lovas Award, the 2022 & 2024 Computers & Composition Michelle Kendrick Award, and grants from the Conference on College Composition and Communication and the Council for Programs in Technical and Scientific Communication.

Contrast the assumed criminality of migrants at the U.S. Southern Border with the recent arrest of Joseph James D'Angelo, the notorious Golden State Killer. Like many high-profile arrests and situations involving police intervention, the capture of the Golden State Killer garnered significant media attention both domestically and abroad not only because numerous decades-long cold cases were solved but also because police revealed they repurposed direct-to-consumer genetics (DTC-genetics) as a rhetorical surveillance technology to identify the serial offender. DTC-genetics are a biometric technology (biometrics) marketed to consumers who want to learn more about their genetic make-up, medical information, or family history without the direct involvement of a licensed healthcare professional. Authorities in California used the DTC-genetics website GEDmatch.com (GEDmatch) to perform genetic testing in the Golden State Killer case. DTC-genetics, here, doubles as a rhetorical surveillance tool within the larger global digital surveillance infrastructure, one supported by and that supports systemic injustices against multiply marginalized bodies and is abetted by unethical surveillance occurring as part of the white supremacist American law enforcement apparatus. The Golden State Killer is the most prolific offender in California state history, and he was a police officer. He is a US citizen, not an immigrant who is always-already assumed to be a criminal. His genetic profile allowed him to avoid capture for decades within our surveillance society; that is, being a cisgender heterosexual white man was a benefit, exempting him from systematic daily surveillance.

Since 2018, DTC-genetics companies like GEDmatch, 23andMe.com (23andMe), and Parabon Laboratories (Parabon Labs) have assisted police with solving cold cases while also empowering racial profiling and contributing to the long history of privacy erosion of Black, Indigenous, and People of Color (BIPOC) in the U.S. In a wide-ranging critique that arrived as privacy erosion caused by the increasing popularity of DTC-genetics was increasing in America, Black feminist Simone Browne demonstrates how biometrics have always been a tool for surveilling Blackness, which she defines as "identity and culture, history and present, signifier and signified, but never fixed," from slavery to today, and are thus a cornerstone of the American law enforcement and criminal justice systems (8). This unethical surveillance strategy has long-lasting, far-reaching social, economic, and political implications which need to be analyzed because genetics as a rhetorical surveillance tool perpetuates discriminatory policing strategies.

State and federal laws both govern and exist in concert with the Terms of Service (ToS) documents governing user interactions and data collection for genetics companies. ToS documents include privacy policies, user agreements, and other policy statements outlining the relationship between a user and a technology, product, or service. Estee Beck explains that privacy policies are written for the express purpose of protecting a company or website from legal damages. In recent years DTC-genetics companies integrated enhanced measures detailing their values regarding data privacy and digital surveillance and their products and services, including updating their ToS documents to offer opt-out protocols and attend to the disparities in legal coverage for users based on their geographic location (geolocation). However, due to the expanded use of biometrics, we must consider how some technologies are designed and repurposed to be beneficial for political, cultural, technological, and educational institutions in the new surveillance (Marx), like in the Golden State Killer case. And perhaps there is no better place to study how biometrics perpetuate systemic oppression and bodily control than at the border(lands)—an imagined geographical and culturally liminal space.[1]

Biometrics are an asset for the global surveillance infrastructure that privileges cisgender heterosexual white able-bodied men. Technofeminist intervention into biometrics is needed because the data that fuels them comes, quite literally, from the body and (re)conceptualizations of the body remain a primary concern of feminist research. As Ann Shivers-McNair, Laura Gonzalez, and Tetyana Zhyvotoyska explain, we must "embrace and enact the interconnectedness of technological practices and gender, race, class, and sexuality, as well as their co-constitution and shaping of each other" (46). Researchers in rhetoric and composition, therefore, need feminist methodologies that amplify intersectionality and that interrogate the *collisions* of asymmetrical power stemming from inequity to study and dismantle this late capitalist phenomenon (Crenshaw).

In this essay, I work toward that goal by building on scholarship defining and extending *digital rhetorical privacy* to *talk back* against unethical surveillance caused by using biometrics for bodily control. I triangulate *digital rhetorical privacy* with Simone Browne's *racializing surveillance* and Morgan C. Banville's *interlocking surveillance* to demonstrate *interlocking consent* as an intersectional paradigm (Collins; Collins and Bilge). Interlocking consent explains the interlocking nature of various ToS policies and amplifies the geo-spatial elements of data privacy erosion and unethical digital surveillance via analysis of the rhetorical surveillance practices used at the U.S. Southern Border. I posit that understanding how biometrics—wherein the body is digitized and datafied—perpetuate oppression from an intersectional technofeminist perspective is a critical rhetorical attunement emphasizing how technologies fueled by the intersection of "the body" and "the digital" contribute to "The Privacy Aesthetic." Finally, I offer necessary paths forward that include negotiating rhetoric's relationship to privacy and surveillance and amplifying the geolocation of data collection practices.

Digital Rhetorical Privacy, Racialized Surveillance, and Interlocking Surveillance

Defining privacy is very difficult because people understand what privacy is but have different ideas about what constitutes it. Estee Beck and Les Hutchinson Campos write that "one of the problems with defining privacy––especially within legal reform––is the utter disharmony in views about the many distinctions of discretion due to varying subject positions and life experiences" (6–7). Understanding privacy erosion amid unethical surveillance across "varying subject positions and life experiences" propels a theory of digital rhetorical privacy, which is a "state of being when a user is confident their digital data is free from unauthorized observances by nefarious computer technologies and other users" (Woods 5). Here, nefarious means looking at the data collected and how it is used. Digital rhetorical privacy accounts for the cultural aspects of the privacy-surveillance continuum to underscore how unethical surveillance supports oppressive social, political,

[1] Gloria Anzaldúa (1987) conceptualization of La Frontera and the body influences how I understand the relationship between biometric technologies and imagined borders.

and economic infrastructures. In this way, such a theory responds to what Patricia Hill Collins describes as the matrix of oppression (or matrix of domination), an understanding of how different characteristics such as race, gender, and socioeconomic status exist simultaneously and why power is distributed asymmetrically throughout society.

The theory of digital rhetorical privacy, as an analytic, originally proposed six inherently intertwined analytic elements to guide the analysis of ToS documents, including (1) temporality, (2) transparency, (3) language, (4) data usage, (5) digital surveillance, and (6) meaningful access (Woods). An incomplete but pliable theory initially, rhetoric, composition, and technical communication scholars have extended digital rhetorical privacy by arguing for innovative pedagogical applications centering remediations of privacy policies (Woods and Wilson), advocating for critical digital literacies for patients using medical wearables (Woods and Wason), and conceptualizing privacy literacy as essential to digital life by focusing on the design of ToS documents (Woods and Johnson).

Here, I argue, digital rhetorical privacy must emphasize its connections to understandings of racializing surveillance. Simone Browne, studying how Blackness is surveilled across space and time, introduces the concept of racializing surveillance as "a technology of social control where surveillance practices, policies, and performances concern the production of norms pertaining to race and exercise 'a power to define what is in and out of place'" (Browne 16; Fiske, quoted in Browne).[2] Placing racializing surveillance in concert with a theory like digital rhetorical privacy re-situates emphasis toward understanding how elements like language and data usage are positioned in ToS documents to perpetuate racism. What jargon and/or legalese regarding geolocation *blurs* values about data privacy and digital surveillance? How do we contend with the *racialization* of data collection outlined in ToS documents? What does it mean to imagine equitable futures when "white adults are more likely than Hispanic and black adults to think it's acceptable for law enforcement to use information from cell phone towers to track people's locations" (McClain et al.)? Further, merging racialized surveillance with digital rhetorical privacy propels robust interrogations of how design and meaningful access keep certain bodies out of places and spaces (Selfe and Selfe; Banks; Woods and Wilson). Importantly, these conversations must be situated within a wider breadth of concerns about consent and biometrics.

Morgan C. Banville introduces interlocking surveillance as a theoretical framework in her study of healthcare professionals' perceptions of consent in medical settings that use biometrics. Interlocking surveillance "combines elements of the new surveillance and intersectionality to develop a framework that addresses sites of surveillance and their levels of awareness, advocacy, and transparency of normalized surveillant practices" (Banville 90). Interlocking surveillance exponentially and categorically enhances a theory like digital rhetorical privacy because it offers a way to understand how ToS documents perpetuate systemic oppression. While Banville develops interlocking surveillance by analyzing intersectional approaches to understanding

[2] *Racializing surveillance* is one of two concepts Browne posits along with Dark Sousveillance, which is "a way to situate the tactics employed to render oneself out of sight, and strategies used in the flight to freedom from slavery as necessarily ones of undersight (21). My focus is on racializing surveillance for this essay.

surveillance in healthcare, I leverage interlocking surveillance to examine more closely the racialized implications of ToS and offer interlocking consent to extend Banville's framework. Ultimately, understanding the interlocking and overlapping nature of the digital rhetorical privacy framework via interlocking surveillance illuminates the interlocking nature of consent. In the following section, I merge racialized surveillance, interlocking surveillance, and digital rhetorical privacy to introduce the concept of interlocking consent through analysis of rhetorical surveillance practices and policies used by the OBIM at the U.S. Southern Border.

Interlocking Consent at the U.S. Southern Border

Combining racialized surveillance and interlocking surveillance with digital rhetorical privacy illuminates the holistic, justice- and equity-oriented efforts underlying the theory. It also foregrounds the importance of understanding what I describe as interlocking consent, a critical intersectional paradigm and additional analytical element for the *digital rhetorical privacy* framework. Interlocking consent demonstrates how consenting to one ToS interlocks with other ToS. As a theory, it values intersectionality and racialized surveillance and seeks to disrupt and dismantle the "practices, policies, and performances" concerning consent that led to racial oppression (Browne 8). Furthermore, interlocking consent values feminist and queer conceptualizations of consent located in the body (Chávez), in sexual experience (Bauer), and in the right to consent (Donovan, Butterby, and Barnes), and, as an analytic element, interlocking consent coalesces with Sasha Costanza-Chock's principles for design justice and provide a path to work against surveilling gender (non)conformity, a hallmark of transgender politics (Beauchamp), abetted via ToS. Importantly, interlocking consent pushes us toward not only policies but also practices for obtaining consent and transmitting data––sometimes across imagined borders where laws governing consent differ.

Critically, a single genetic sample is used in different ways in the Immigration Detention Centers at the U.S. Southern Border, which illuminates the multipurpose nature of data usage and the importance of understanding interlocking consent. Genetic samples are sent to the federal Combined DNA Index System (CODIS) *and* used for rapid testing to determine familial connections. The DHS is a critical component of the larger American law enforcement apparatus, and the interlocking ToS documents and policies, laws, and practices governing the use of facial recognition software, global positioning systems (GPS), aerial drones, genetics, and other biometrics used for bodily control at the U.S. Southern Border necessitate intersectional technofeminist intervention. DHS positions biometrics as helpful: "Biometrics collected by DHS and linked to specific biographic information enable a person's identity to be established and then verified" (DHS). DHS highlights the ability to identify "suspected terrorists, criminals, and immigration violators" using biometrics to ensure that [a] document belongs to the person presenting it" (DHS). Interlocking consent offers us a way to understand these policies and practices as oppressive at this critical rhetorical surveillance site (Lyon). When we consider the implications for data privacy and digital surveillance at the U.S. Southern Border, we must ask: How do immigrants coming to the U.S. Southern Border consider the implications of their interlocking consent when they submit their genetic sample in hopes of entering the U.S.? Do you think you would care about your interlocking consent in that spacetime?

Examining interlocking consent related to genetic technologies at the U.S. Southern Border amplifies previous arguments about the constellation of policies users must navigate, often via hyperlink, to understand how data collected might be used (Woods and Wilson). It illuminates the complex, multipurpose use of digital data collection and the importance of understanding how consent to data collection via a product or service––or in the case of immigrants, a requirement for border crossing––can (and does) lead to its use in other contexts. For example, the OBIM "Biometrics" webpage on the DHS website prompts users to learn more about topics like "Exchanging Biometric Data" and "Privacy Information" in their navigation panel. Including these two webpages denotes to users that biometric data collected at the Southern Border will be exchanged among various stakeholders and third parties. Biometric data potentially shared includes Unique Person Identifiers, photographs and fingerprint information, and the different organizations which might have access to this data via the Automated Biometric Identification System (IDENT) includes, but is not limited to, the Federal Bureau of Investigation (FBI) Next Generation Identification (NGI) System, the Department of Defense (DoD) Automated Biometric Identification System (ABIS) and the international community via the Secure Real-Time Platform (SRTP). This necessitates the development of interlocking consent.

The webpage for "Privacy Information" includes contact information and Freedom of Information Act (FOIA) information alongside a "Privacy Mission Statement" that reads:

> The mission of the OBIM Privacy Office is to uphold the privacy of people while protecting our national borders. We do this by adhering to the letter and spirit of U.S. privacy laws, complying with fair information practices (notice, choice, access, security and redress), by treating people and their personal information with respect and by ensuring a high standard of privacy protection.

It is difficult to define privacy in the United States, even with foundational laws and especially amid evolving data privacy legislation. Further, the politically polarized state of the republic—evidenced by Donald Trump's *migrant crime* comment—defies the notion that Americans maintain a comprehensive spirit regarding privacy laws in the country. How can the DHS purport a high standard of privacy protection if data is shared among various governmental organizations and third parties without consent, let alone the fact that DHS cannot preserve immigrant families by keeping family members together throughout the immigration process? Finally, and importantly, necessitating users to comprehend "Privacy Information" by giving the topic its own navigable webpage and developing a Privacy Mission Statement for the OBIM website amplifies what I describe as *The Privacy Aesthetic*.

The Privacy Aesthetic

A defining feature of our current surveillance capitalist moment includes people's interlocking attitudes, beliefs, and values about, and ideologies, epistemologies, and aesthetics regarding data privacy and digital surveillance as society contends with the infrastructural saturation of digital surveillance technologies (Zuboff). By infrastructural saturation, I am referring to the analog and digital technologies, policies, and practices that influence our existence by propelling a predisposition for considering data privacy and digital surveillance, and which prompt a reorientation to "the digital" as "a multisensory, embodied condition" absent "even the most innocuous of activities, such as grocery shopping, now rely on computational procedures that connect local purchases to global supply chains" (Boyle et al. 252). These include new surveillance technologies like Closed-Circuit Television (CCTV), surveillance cameras and body cameras (body cams), facial recognition software, GPS, aerial drones, and DTC-genetics, among others (Marx). Infrastructural saturation also includes ToS documents and their features, like pop-up and dialogue boxes that prompt user agreement, and the Cookie policies users must acknowledge on websites that seek traffic from users who are in the EU, which is governed by the GDPR. It is not difficult to understand how infrastructural saturation of surveillance technologies are influencing our lived experiences in real time. For example, we can analyze how *dark sousveillance* occurs during Black Lives Matter protests and how women like Brittany Watts must make critical decisions about maternal-fetal health in states that do not value maternal-fetal health (Browne). And, of course, we can look to the immensely vast and ever-expanding network of Borderveillent infrastructures implemented for bodily control at the U.S. Southern Border (Fojas). Ultimately, these contribute to a wider aesthetic for understanding privacy and surveillance: The Privacy Aesthetic.

By *aesthetic* (or aesthetics) I am referring to design features but also the capacity for design features to guide a movement towards valuing privacy in different (side)ways. Immigrants who arrive at the U.S. Southern Border are acutely aware of the importance of their geo-spatial orientation and likely aware of the hyper-politicization of their body, as well as the critical influence of privacy and surveillance on their lives. When they submit their genetic sample to CODIS and for rapid testing, a condition of their entrance into America, they are submitting a powerful and proven biopolitical biometric. But what about other emerging technologies, like collecting biometric data from drones equipped with facial recognition? What happens when biometric data is collected via drones that then traverse imaginary geographical borders for uncertain purposes with deep sociopolitical consequences? In her work, artist Dinie Besems explores privacy as a luxury and how we divulge devices into our private spaces. Designer Jesse Howard values privacy in the redesign of digital technologies. In coordination, artist Tijmen Schep outlines eight principles coalescing around security and authenticity:

1. privacy first
2. think naughty
3. collect as little data as possible
4. protect your data
5. understand identity
6. open the black box

7. make the user a designer
8. technology is not neutral.

The Privacy Aesthetic I describe is a positive technical consideration that aligns with these eight principles to contend with privacy erosion occurring at the U.S. Southern border. The Privacy Aesthetic also includes an attunement to the oblique ubiquity of rhetorics of privacy and surveillance (Boyle); recognition of ToS documents as one of the most influential genres in the world (Woods); cognizance of the intersection of "the body" and "the digital" as essential for new surveillance technologies to maintain their influence; and consideration of the importance of geolocation regarding data collection.[3]

The triangulation of aesthetics with privacy and surveillance is not a new or novel approach to understanding culture. Michel Foucault conceives us "at a moment when the world is experiencing…something less like a great life that would develop through time than like a network that connects points and weaves its skein" (175). The Privacy Aesthetic is an orientation "now appearing on the horizon of our concerns, of our theory, of our systems" and it maintains "a history, and one cannot fail to take note of this inevitable interlocking of time and space" (Foucault 175–176). More recently, Casey Boyle argues, "As the field moves the needle of inquiry well beyond ways humans use symbolic language for communication, whole waves of thinking call us to surrender head-on modes of engagement in favor of sideways means of knowing and elliptical ways of being and moving" (68). The Privacy Aesthetic favors "sideways means of knowing" and "emphasizes elliptical ways of being and moving" that contend with infrastructural saturation and offers a renewed approach to overcoming collective apathy about privacy and surveillance, which is often initiated in ToS documents. Saturation as a catalyst for apathy necessitates a turn "to and with aesthetics as other-than-direct orientations offer other ways to transverse recent concerns over ontology and epistemology" (Boyle 69). Thus, The Privacy Aesthetic represents a move from analysis to aesthetics–from a privacy rhetoric to a privacy aesthetic.

Ultimately, The Privacy Aesthetic I describe stratifies an oblique orientation to pressing ontological concerns and seeks to deconstruct dominant and oppressive epistemologies regarding ubiquitous privacy and surveillance. By oblique, I am referring to, as Boyle does, a "function concern[ed] not only the material design of structures but also the affective possibilities capacitated by embodied experiences when practicality and something like playfulness coincide (68). Emphasizing obliqueness elucidates the asymmetrical power of data privacy and digital surveillance and presses us to consider the increasing interfacing of "the body" and "the digital" as inevitable.

[3] Blurring humanity and technology is a post-humanist concern, certainly, but fully articulating the influence of post-human technologies beyond biometrics is beyond the scope of this essay.

Necessary Paths Forward

In this essay, I explained the impetus for analyzing biometrics: the implementation of DTC-genetics into the American law enforcement apparatus, especially at the U.S. Southern Border where immigrant populations are coded not as future citizens but future criminals. Using DTC-genetics as a tool of surveillance in law enforcement produces negative implications for bodies that are already disproportionately and negatively impacted, particularly Black bodies and immigrant bodies. Additionally, I engaged with racialized surveillance and interlocking surveillance to introduce a new paradigm and analytical element into the digital rhetorical privacy framework: interlocking consent. Future studies centering interlocking consent will require intersectional interrogations if we are to overcome the norms of oppression stemming from social sorting (Dubrofsky and Magnet; Browne, Banville). The Privacy Aesthetic, as a concept linked to interlocking consent, is a means of amplifying rhetoric's relationship to the privacy-surveillance continuum and the importance of the geo-spatial element of data collection. Perhaps a primary offering of rhetorical approaches to understanding privacy and surveillance is emphasizing the deconstruction of the faux privacy "and" surveillance binary and the merging of the two onto a comprehensive privacy-surveillance continuum for newfound and renewed issues like the widespread adoption of AI, as we navigate living in a world with Coronavirus, amid the passage of oppressive legislation regarding bodily autonomy, and as America reckons with immigration reform at the U.S. Southern Border.

We, technofeminist scholars in rhetoric and composition, must continue using emerging theoretical frameworks to interrogate complex data privacy and digital surveillance strategies outlined in ToS. A pliable theory like digital rhetorical privacy offers additional opportunities for expansion beyond engagements with Browne's racialized surveillance and Banville's interlocking surveillance theories in the analysis of biometrics used at the U.S. Southern border in this essay. Future directions should consider the geolocation of data collection and automation and advocate for equitable futures defined by a tactical privacy. Further research should engage with how ToS contribute to Anthony Stagliano's disobedient aesthetic and, while the focus of this article was on biometrics, researchers should engage, like Iván Chaar López has, with the uniqueness of aerial drones in relation to intrusion. We must consider: Where was the data collected, and what laws govern data privacy and digital surveillance there? Was data transferred across imagined borders of states and countries where laws governing data privacy and digital surveillance differ? And where does that data go after it is collected? How is it moved through oppressive digital and legal networks? These are essential questions for technofeminists invested in resisting asymmetrical power, combatting privacy erosion, and safeguarding bodily autonomy.

Works Cited

Anzaldúa, Gloria. *Borderlands/La Frontera: The New Mestiza*. Spinsters/Aunt Lute, 1987.

Banks, Adam J. *Race, Rhetoric, and Technology: Searching for Higher Ground*. Routledge, 2006.

Banville, Morgan C. *Am I Who I Say I Am? The Illusion of Choice: Biometric Identification in Healthcare.* 2023. East Carolina University, PhD dissertation.

Bauer, Robin. "Queering Consent: Negotiating Critical Consent in Les-Bi-Trans-Queer BDSM Contexts. *Sexualities*, vol. 24, no. 5–6, 2021, pp. 767–783, doi.org/10.1177/1363460720973902.

Beauchamp, Toby. *Going Stealth: Transgender Politics and U.S. Surveillance Practices*. Duke UP, 2019.

Beck, Estee. "Who Is Tracking You? A Rhetorical Framework for Evaluating Surveillance and Privacy Practices." *Establishing and Evaluating Digital Ethos and Online Credibility*, edited by S. Apostel and M. Folk, IGI Global, 2016, pp. 66–84, doi.org/10.4018/978-1-5225-7113-1.ch015.

—, and Les Hutchinson Campos, editors. *Privacy Matters: Conversations about Surveillance within and beyond the Classroom*. UP of Colorado, 2020.

Boyle, Casey. "The Unbearable Obliqueness of Rhetoric." *Rhetoric Society Quarterly*, vol. 54, 2024, pp. 68–73, doi.org/10.1080/02773945.2023.2236998.

—, James J. Brown Jr., and Steph Ceraso. "The Digital: Rhetoric Behind and Beyond the Screen." *Rhetoric Society Quarterly*, vol. 48, no. 3, 2018, pp. 251–259, doi.org/10.1080/02773945.2018.1454187 .

Browne, Simone. *Dark Matters: On the Surveillance of Blackness*. Duke UP, 2015.

Chávez, Karma R. "The Body: An Abstract and Actual Rhetorical Concept." *Rhetoric Society Quarterly*, vol. 48, no. 3, 2018, pp. 242–250, doi.org/10.1080/02773945.2018.1454182.

Costanza-Chock, Sasha. *Design Justice: Community-Led Practices to Build the Worlds We Need*. MIT Press, 2020.

Crenshaw, Kimberlé. *On Intersectionality: Essential Writings*. The New Press, 2017.

Department of Homeland Security. *Biometrics*. Accessed 19 July 2024, https://www.dhs.gov/biometrics.

—. *Exchanging Biometric Information*. Accessed 19 July 2024, https://www.dhs.gov/exchanging-biometric-data.

—. *Privacy Information*. Accessed 19 July 2024, https://www.dhs.gov/biometrics.

Donovan, Catherine, Butterby, Kate, and Barnes, Rebecca. "'I wasn't aware at the time, I could actually say "no"': Intimacy, Expectations, and Consent in Queer Relationships." *Consent: Legacies, Representations, and Frameworks for the Future*, edited by Sophie Franklin, Hannah Piercy, Arya Thampuran, and Rebecca White, Routledge, 2023, pp. 154-169.

Dubrofsky, Rachel E., and Shoshana A. Magnet, editors. *Feminist Surveillance Studies*. Duke UP, 2015.

Fiske, John. "Surveilling the City: Whiteness, the Black Man, and Democratic Totalitarianism." *Theory, Culture, and Society*, vol. 15, 1998, pp. 67–88, doi.org/10.1177/026327698015002003.

Fojas, Camilla. *Border Optics: Surveillance Cultures on the US-Mexico Frontier*. NYU Press, 2021.

Foucault, Michel. "Different Spaces." *Michel Foucault: Aesthetics, Method, Epistemology*, edited by J.D. Faubian, The New Press, 1984/1994, pp. 175–185.

Hill Collins, Patricia. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. 2nd ed., Polity Press, 2008.

Hill Collins, Patricia, and Sirma Bilge. *Intersectionality*. 2nd ed., Polity Press, 2020.

hooks, bell. *Talking Back: Thinking Feminist, Thinking Black*. South End Press/Routledge, 1989/2015.

López, Iván Chaar. *The Cybernetic Border: Drones, Technology, and Intrusion*. Duke UP, 2024.

Lyon, David**.** *Surveillance Studies: An Overview*. Polity Press, 2007.

Marx, Gary T. "Ethics for the New Surveillance." *The Information Society*, vol. 14, 1998, pp. 171–185, doi.org/10.1080/019722498128809.

McClain, Colleen, Michelle Faverio, Monica Anderson, and Eugenie Park. "How Americans View Data Privacy: The Role of Technology Companies, AI and Regulation – Plus Personal Experiences with Data Breaches, Passwords, Cybersecurity and Privacy Policies." *Pew Research Center*, 18 Oct. 2023, https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

Schep, Tijmen. *Design My Privacy: 8 Principles for Privacy Design*. Laurence King Publishing, 2016.

Selfe, Cynthia L., and Richard Selfe. "The Politics of the Interface: Power and Its Exercise in Electronic Contact Zones." *College Composition and Communication*, vol. 45, no. 4, 1994, pp. 480–504, https://jstor.org/stable/358761.

Shivers-McNair, Ann, Laura Gonzales, and Tetyana Zhyvotovska. "An Intersectional Feminist Framework for Community-Driven Technology Innovation." *Computers and Composition*, vol. 50, 2019, pp. 43–54, doi.org/10.1016/j.compcom.2018.11.005.

Stagliano, Anthony. *Disobedient Aesthetics: Surveillance, Bodies, Control*. U of Alabama P, 2024.

Woods, Charles. *Interrogating Digital Rhetorical Privacy on Direct-to-Consumer Genetics Websites*. 2021. Doctoral dissertation, Illinois State University.

—. "ChatGPT and Privacy." ChatGPT, Magical Thinking, and the Discourse of Crisis,

Conference on College Composition and Communication, 17 February 2023, Chicago Hilton, Chicago, IL. Special Session.

—, and Noah Wilson. "The Rhetorical Implications of Data Aggregation: Becoming a 'Dividual' in a Data-Driven World." *The Journal of Interactive Technology & Pedagogy*, vol. 19, 2021. https://jitp.commons.gc.cuny.edu/the-rhetorical-implications-of-data-aggregation-becoming-a-dividual-in-a-data-driven-world/.

—, and Noah Wason. "Making Well-Informed Decisions: Data Collection, Health Information, and Undergraduate Writing Instruction." *Composing Health Literacies: Perspectives and Resources for Undergraduate Writing Instruction*, edited by Michael Madson, Routledge, 2023, pp. 195–206.

—, and Gavin P. Johnson. "(Re)Designing Privacy Literacies in the Age of Generative AI." *Toward Digital Life,* special issue of *Communication Design Quarterly,* vol. 12, no. 2, 2024, pp. 86–97.

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. Profile Books, 2019.