Pervasive Practices: Pedagogical and Programmatic Influence of Biometric Technologies as Surveillance

Morgan Banville
Massachussetts Maritime Academy

Abstract: Introducing students in higher education to issues of surveillance within technical and professional communication courses creates an opportunity to reflect, analyze, and interrogate students' digital literacies. This article contributes to imagining what the creation of a technical and professional communication course that centers topics and common issues in surveillance studies may look like. The article includes foundational readings, example assignments, and a case scenario that guides students in exploring how surveillance impacts their daily lives. Due to the global rise in digital privacy and surveillance concerns, as well as increasing implementation of emerging technologies in various sectors, this article argues that higher education courses should implement issues involving surveillance as a core learning outcome.
Keywords: technical and professional communication, surveillance, biometric technology, privacy, data

An Exigency for Intervention[1]

Surveillance is a key writing and thinking activity that impacts our day-to-day lives in a multitude of ways; this article guides instructors across disciplines and institutions in its impact within the technical and professional communication (TPC) classroom space. One of the roles of technical communicators, functioning as knowledge-makers, creators, and instructors, is to communicate with audiences regarding how surveillance impacts their daily lives. Since technical communicators are advocates (Jones, 2016; Walton, Moore, & Jones, 2019), then advocating for historically excluded and multiply marginalized individuals and groups becomes an important part of a technical communicator's teaching. Instructors should discuss with students how and why bodies are impacted by surveillance technologies and implement programmatic and

1 As a condition of the grant received to pay nurses from the Council for Programs in Technical and Scientific Communication, this article is revised from Chapter 6 of my dissertation study.

Contact Author: morgancbanville@gmail.com

pedagogical initiatives to contend with topics such as digital and civic literacy, and design.

This article extrapolates pedagogical and programmatic takeaways from a year-long research study. Grounded in surveillance studies and technical communication, I define biometric identification technologies as personal identifiers of the body (Banville 2023). The following suggestions, resources, and content derives from a study that answered: What are neonatal nurses' usages and perceptions of biometric technology in healthcare? To answer the research question, I explored the connection (or tension) between neonatal nurses' perceptions and usage of biometric technology in healthcare, and the communication materials developed by biometric solution companies. The study focused specifically on how neonatal nurses use and perceive such technologies within the context of the United States healthcare system. The study was conducted in three parts: I compiled a corpus of communication materials from biometric companies, distributed questionnaires, and conducted ten interviews with neonatal nurses. The study found that major themes (convenience, safety, security/compliance) from the data collection can be fruitful for implementation into the technical communication classroom (see Banville, 2023). To assist with providing context for the scope of this article, the following are the results and takeaways of this study:

- Technical communicators are not just those who create documents or design web content. Neonatal nurses are technical communicators: they communicate and negotiate specialized information. We can further redefine what it means to be a technical communicator.
- Technical communicators can engage in a participatory approach between those who create communication materials, and those who implement it. This is necessary to attend to issues of security, compliance, and efficiency in healthcare.
- Technical communicators and designers of biometric technologies should articulate cultural, political, and biomedical realities in its activist discourse.
- Technical communicators can engage in the design process through participation, and informing biometric companies about the ways they may actually communicate informed consent, even if "opting out" is not an option.
- Technical communicators can engage in the ethical design of the technology, but we also need to advocate for awareness (through proper informed consent) and transparency of data collection practices.
- Technical communicators can intervene in the tradeoff fallacy[2] and privacy paradox[3] through the creation and design of materials that communicate transparently (through localizing knowledge) about privacy, data, and surveillance concerns.
- Technical communicators can intervene in the design of both texts and technologies.

2 The false misconception that Americans are aware of their data collection, especially as it relates to surveillance in healthcare.

3 The privacy paradox refers to the "conflict between individuals express[ing] concern over privacy and their apparent willingness to surrender that privacy in online spaces in exchange for very little of value" (Colleen Reilly, 2021, p. 33).

One takeaway that may be of interest to TPC programs is how biometric companies communicate their products to consumers emphasizing efficiency, compliance, and safety, often without accounting for a person on the other end of and/or using the technology. The neonatal nurses interviewed in my study adopted language based on the communication materials used for training(s) in the healthcare setting, which were very similar to the language on the biometric websites themselves. Similar to what Isidore Dorpenyo (2022) found in their analysis of documents, the corpus I collected also encouraged users to constantly engage the specific biometric solution, suggesting task-oriented instructions and language that, in this study, would then be communicated to patients. These styles are adopted to enable users "to quickly and efficiently complete the task at hand" (Seigel, 2013, p. 71). Such documents ultimately make a case for why it is necessary to adopt biometric technologies: convenience, safety, and/or compliance.

Biometrics as Surveillance: An Intersection with TPC

Despite the poised necessity of convenience, safety/security, and compliance, the themes are useful to use in the TPC classroom to guide students in considering how to approach design and critical analysis of emerging technologies. Such themes and takeaways, such as convenience, safety, and compliance, are foundational to guiding and shaping the sample implementation of resources into the TPC classroom, as design and documentation is of particular importance and interest to students studying in technical and professional communication.

Convenience

As instructors, scholars, and participants in society we must prepare students to enter the workforce, addressing the purpose of implementing biometric technologies, how they are defined, and the ethical implications such as who they protect and harm. For example, the concern with data privacy has recently extended to focus on biometric usage in social media. TikTok's CEO Shou Zi Chew explained that the social media application determines the age of its users by scanning videos (Perez, 2023). This feature is labeled as convenient for parents/guardians [and the company] to monitor age restrictions. However, as TPC instructors, we may encourage students to ask follow-up questions to this example such as what specific facial recognition or other technologies TikTok uses, and whether those technologies were "built in-house" or if the company relies on "facial recognition tech built by third parties" (Perez, 2023). Efficiency/Convenience, which technical communicators have extensively critiqued (Frost, 2016; Scott, Longo, & Wills, 2006), often refers to the ability to complete or produce something quickly without wasting materials, time, or energy.

Emerging technologies are designed to make a task "easier" or convenient. An article written by Senior Product Designer Taras Savytskyi (2022) documented the reasoning behind the design of the origin story of Sony Walkman, Mini Cooper, and the iPhone. How does this relate to biometric technologies? The research and vision are the same: create technologies for ease of use and access. Savytskyi (2022)

writes about the Mini, "Every decision they made during the build phase was aimed at saving space and improving efficiency" (n.p.). Instructors can use biometric technologies to exemplify why data privacy is so important; including discussions of past and emerging technologies' being introduced as convenient.

Safety and Security

With some of the 'positive' aspects of biometric technology poised by corporations and mass media alike, it can be difficult to think past the sometimes-invisible implications of such technologies. Often, these shiny, new technologies are poised as a means for additional "convenience" or "efficiency," or even "safety." A quick Google search asking "why use biometric authentication" provides a long list of webpages advocating for verification of identity, their convenience, added security measures, and an emphasis on faster authentication (or efficiency) (see Figure 1). Security is defined as protection or measures taken to guard against unauthorized entities from accessing information, accounts, or other personal information.

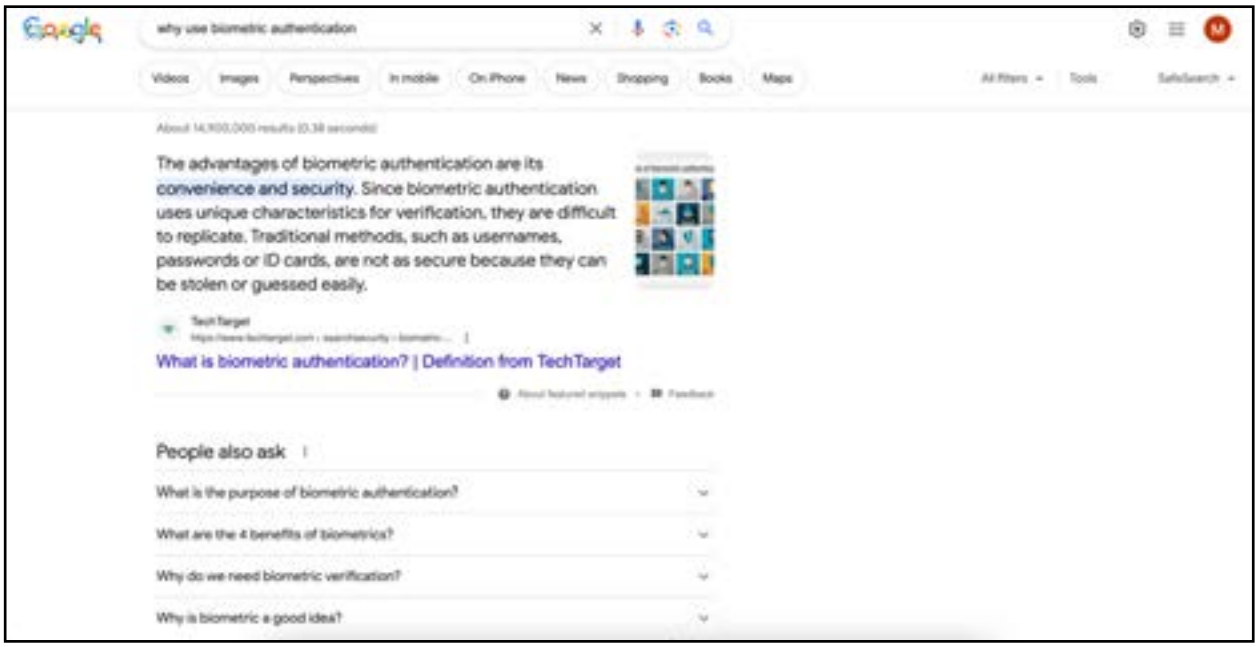

Figure 1: Example screen-capture taken on December 28, 2023

One doesn't need to look too far to witness numerous examples of biometric usage paraded as secure and efficient in the consumer arena: a study from 2017, for example, suggested that "70 percent of consumers believe that biometrics are easier, and 46 percent think they are more secure than using passwords or PINs " (Visa, 2017). There are increasing introductions of biometrics into the consumer space; however, the classroom space is one site of intervention where students can help to consider the implications of who the technology is identifying, protecting, harming, and how such are implemented. Oftentimes biometric technologies are not just used for identification, but also for securing information. There is a huge disconnect between the perception of safety and security, and the actual implementation of such. Where does the information go? How is it stored? What third-parties or other parties have access to this information? What can they

do with the information? There are gaping holes in the links between what is perceived safety, versus true security. And this is the problem with deceptive design. Deceptive design, also known as "dark patterns," is commonly referred to as tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something (Brignull, 2023). Isidore Dorpenyo (2019) mentions how technical communicators should consider the socio-cultural context surrounding when/where the biometric technologies are used. This would mean considering aspects such as "weather conditions, spatial relations, knowledge of users, social practices of users, the nature of work in which users are engaged, and how the work they do might affect successful use of the technology" (Dorpenyo, 2019, p. 373). Such socio-cultural conditions can affect the ways in which biometrics may deceive users and authentication/identification processes, impacting their safety/security and deeming them 'non-compliant.'

Compliance

The way biometric companies discuss convenience, security/safety, and compliance as well as how they define biometric identification, and the respective technology is a component of digital literacy in the technical communication classroom. For example, security firm BioCatch provides tools for companies to "learn employees' digital behavior and identify when an unauthorized person is trying to access information" (Larson, 2018). Companies can add BioCatch software to apps and websites. It runs in the background to build a 'behavior profile' of a user, and "learns activities like how someone holds the phone, whether they type with one or two hands, and how they scroll or toggle between screens" (Larson, 2018). Students should be aware of the ways in which they may be 'required' by companies to act in certain ways to be "in compliance." Compliance generally refers to following set rules, regulations, and laws that relate to practices. Compliance is often discussed in terms of safety, specific standards or procedures, and ultimately risk management. Compliance therefore regulates; surveillance tools such as biometric technologies exacerbate compliance initiatives in the ways that the technology becomes an embodiment of the person. Are you who you say you are? If you do not consent to use the technology, are you non-compliant? In the TPC classroom, students can approach understanding compliance as always contextual. Further, compliance is not always positive (or always negative). Discussing biometric technologies as they relate to compliance prepares students for the emerging technologies they may encounter in the workplace, as well as how to navigate such technological implementation. For example, a medical patient who is willing to comply but whose circumstances prevent complete adherence to a protocol is out of compliance: their (willing) attitude is at odds with their (noncompliant) (in)actions, their intentions out of alignment with the effects of such actions (Banville, Clark, and Sharp-Hoskins, 2025).

Administrators and instructors in technical and professional communication can utilize biometric technologies as a relevant example in understanding sites of surveillance. The focus in the curriculum might emphasize how biometric companies position themselves and their product (through communication materials), as well as students exploring what they perceive the role of a technical communicator to be in this exchange. Themes such as convenience, compliance,

safety and security, are of interest to technical and professional communication (TPC) programs across the globe and can be used to guide curriculum and class discussions. My course proposal is specific to the United States, however, global TPC undergraduate and graduate programs could also benefit from introducing issues related to surveillance, data privacy, and informed consent, as they relate and impact communication and design materials in various industries.

Programmatic Promise: A Biometric Revolution

I propose that upper-level technical and professional communication courses across institutions would benefit from critically analyzing and studying biometric technologies as influential and integral to defining the role of technical communicators (and subsequently, the field of technical communication broadly construed). As Oriana Gilson (2021) explains, many students will enter professions that help shape who is able to "access, use, enjoy, contribute to, and interact with online material" (p. 179). These same students view technologies as neutral and unbiased, which is why curriculum should be developed as a "site for action and an area for enacting theory; it is a nurturing ground for critical, functional, and socially just technical communication" (Agboka & Dorpenyo, 2022, p. 60). Technical communication programs and curricula must be sites for engaging social justice issues and enabling students to critique and address systemic inequalities and disadvantages.

The following resources outline how surveillance studies may intersect with technical communication and social justice in the classroom, with the goal "to address issues of power and agency as they manifest in communicative practices and texts" (Jones, 2016, p. 343). This article adds to understanding(s) of how instructors may expose students to "everyday issues of injustice that affect students or in which technical communication might play a role" (Agboka & Dorpenyo, 2022, p. 62). I use the following questions to guide my resources and curriculum:

- How do (and can) technical communicators communicate and design surveillance technologies in industries that reflect students' interest and trajectories?
- How do technical communicators advocate for and resist emerging technologies and their disproportionate hyper-surveillance and impacts on bodies?
- How do technical communicators intervene in their respective roles?

Social justice approaches to TPC are "practical and applied" not merely "theoretical or ideological stances," thus critically analyzing and creating action plans to address emerging technologies is a crucial component of the technical communication class and curriculum (Rebecca Walton & Godwin Agboka, 2021). Biometric surveillance is not just enacted as routine surveillance, but also within other systems, contexts, and institutions including higher education. This article includes example materials such as assignments, reading list(s), and a case example that explores ethical considerations and technology as they manifest in sites of surveillance. In the courses or lessons, whichever instructors decide, students will

be able to consider the ways surveillance is integral to many of our foundational structural systems, "ones that breed disenfranchisement, and that continue to be institutionalized" (Dubrofsky & Magnet, 2015, p. 7). Surveillance practices and technologies normalize and maintain whiteness, able-bodiedness, capitalism, and heterosexuality (see hooks, 1994). The curriculum itself has practical application(s) especially as surveillance technologies such as biometrics have increased as a result of the COVID-19 pandemic, which makes it a useful and timely example to translate into technical communication classrooms across the United States.

Biometric Surveillance in the TPC Classroom

Our goal as educators and users is to empower ourselves and our students to be well-informed citizens. Technical communication instructors and administrators (broadly defined) may be interested in introducing topics of surveillance and privacy within technical communication programs. The following sections outline the ways in which biometric surveillance may be introduced to technical and professional communication classrooms. First, biometrics can be discussed in terms of surveillance and its complex history, especially over the past couple of decades. Further, biometrics can be discussed in terms of their perceived justice, and subsequent injustice. Combining these approaches informs the next section, which outlines a sample course overview.

Surveillance and Complex Histories

Instructors cannot discuss biometric surveillance in theory and application without spending time discussing the history of surveillance. The connotations of surveillance are largely nefarious, complicated by the ways in which surveillance is poised as a "necessity" for "security" and "safety"; students will notice this overlap in communication about biometrics as surveillance tools, as well. Public response is often to dismiss issues of surveillance, security, and privacy; however, as writers, professional and technical communicators, and members of society, it is important to understand how we may become more empowered citizens. One way we may equip our students to become more empowered is by understanding the impact of surveillance technologies in our lives, in our writing, and in our practices. In this area, we can ask:

- What is the purpose of implementing such technologies? Why was this technology initially created, and what is its modern use?
- Who do they protect and harm?
- What are the ethical implications?

Biometric (In)Justices

When we, as instructors and technical communicators, teach about technical communication, biometric technologies, and social justice, we also need to address the ways in which emerging and past technologies (digital and not) have become complicit in injustice. As Dorpenyo (2022) has noted, technical communication about technology has continued to maintain and reproduce "dominant narratives about technology while it obscures and delegitimizes the knowledge of unenfranchised/disenfranchised groups" (p. 292). As such, TPC classrooms may

be structured to consider biometric technologies as an example of how and why communication surrounding emerging technologies has severe implications. For example, students might learn about the "social justice turn" in TPC (Walton, Moore, and Jones, 2019), using biometric influence to explore how certain groups are hyper-surveilled over others through the linguistic and rhetorical choices we make. Kelly Gates (2011) has argued that in surveillance studies advocating for privacy rights can be viewed as problematic. Rachel Hall points to how "welfare recipients, people living in poverty, and queers have never been entitled to privacy," as well as the fact that privacy has not always kept people, especially women and children, safe because violence "often occurs in the home" (2015, p. 149).

Solely focusing on privacy as the only concern related to surveillance and biometrics is a narrow scope that often obscures other pressing concerns. Students in the TPC classroom may consider the ways in which people in various situated contexts have the ability to "opt in/out." Hailey Reissman (2023) posits that because so many Americans view internet privacy as near to impossible to comprehend—with "opting-out" or "opting-in," biometrics, and VPNs—they don't trust what is being done with their digital data. For example, opting in/out presupposes three claims: that people are informed; that they understand what is happening to their data; and that they've provided consent for it to happen (Reissman, 2023). Instructors may use this example to bridge the digital and informational literacy gap to an action plan for students outside of the classroom space. For example, more than 8 in 10 Americans believe, incorrectly, that the federal Health Insurance Portability and Accountability Act (HIPAA) stops apps from selling data collected about app users' health to marketers (Reissman, 2023). Along with privacy concerns, an even larger concern is based on how biometric technologies are impacting people disproportionately, a conversation instructors could initiate with students:

- Why do we need to identify, or authenticate our bodies?
- Why do we need technologies for ease of use, when we know they are fallible and discriminatory?

This brief overview and introduction to biometrics as surveillance technologies informs the following example course, as well as potential outcomes and assignments that instructors could use in the TPC class and/or curriculum and assessment design.

Example Course Overview, Outcomes, and Assignments

Course Overview

In the course—which can be adapted as needed for an undergraduate or graduate curriculum—instructors will examine sites of surveillance as they relate to professional and technical writing. Examination of such sites of surveillance (such as healthcare, the classroom, and other spaces we commonly occupy) will focus on the ways in which emerging (and past) technologies (digital and not) hyper-surveil bodies, predominantly those who are Black, people of color, Indigenous, disabled, and LGBTQIA+. We will read and respond to topics including (but not limited to), algorithmic bias, disability and AI, data mining, surveillance capitalism, privacy, and more. This course will emphasize critical reading, writing, and listening to scholarly

and popular texts that center historically excluded and silenced voices. Assignments will include original research writing; responses to readings, case scenarios, and peer writing; collaborative discussions; and multimodal projects.

Students will rhetorically analyze sites of surveillance as they relate to professional and technical writing and their career goals/trajectories, responding to them in socially relevant ways (including various modes/mediums of response, recognition of language other than Standard Written English, and more) for a range of audiences. Some curriculum guiding questions may explore[4]:

- What is surveillance, and how does it impact technical communicators?
- How, as digital users and technical communicators, does surveillance (and tools, such as biometric technologies), impact professional writing?
- What are the implications of surveillance for historically excluded groups such as those who are marginalized due to race, class, gender, sexuality, and disability?

To align with the curriculum guiding questions, learning outcomes may be adapted as follows.

Learning Outcomes[5]:

Students will…

- Learn how emerging technologies such as biometrics impact groups of people within specific sites of surveillance as they relate to students' future career paths and interests.
- Acquire a conceptual toolkit for analyzing issues related to technology, accessibility, and social justice, as they relate to technical and professional communication.
- Gain experience collaborating with other students to investigate the political, social, cultural, and economic impacts of emerging technologies.
- Analyze both explicit and implicit messages in professional documents.
- Think rhetorically about one's own writing choices and those of others.
- Identify bias and consider its implications in professional and organizational spaces.
- Write for multiple audiences and purposes and in multiple media contexts.
- Communicate effectively, ethically, and responsibly.
- Demonstrate skills, strategies, and conceptual knowledge and practices related to composing and communication tasks (research, revision, collaboration, editing, organization, design, etc.)
- Theorize a variety of reasons, using rhetorical language, for why a responsibility to the public is important for professionals in order for their writing practice to be useful and effective.

Since this course focuses on the intersections of surveillance studies and technical communication, the readings will reflect the specific ways that students (technical

4 This could, and should, be an interdisciplinary course that reflects students' interests.

5 Adapted from Torin Monahan's Technology & Social Justice Course, 2022. I would also suggest reading Monahan's latest book, *Crisis Vision: Race and the Cultural Production of Surveillance*.

communicators) may intervene in their respective career-paths to address issues of surveillance and biometric implementation. The readings will be assigned during thematic weeks, which may include: Power and Legitimacy; Disability and AI; Design and Usability; Healthcare Inequities; Surveilling the Classroom, and more.

To give students an introduction to both technical communication and surveillance studies, I compiled the following assigned readings based on readings that I found especially helpful for grounding work during my own comprehensive exam process as a graduate student. For example, within the intersections of technical communication and surveillance studies, there is only one edited collection (Privacy Matters: Conversations about Surveillance Within and Beyond the Classroom), and one monograph (Working through Surveillance and Technical Communications). Despite this, other than the assigned list, important insights about surveillance have been made by scholars of rhetoric. Researchers have investigated:

- Surveillance as a gaze (Erin Clark Frost & Angela Haas, 2017),
- Data aggregation and commodification (Charles Woods & Noah Wilson, 2021),
- Technological impacts on race and gender (Ruha Benjamin, 2019),
- Wearables (Morgan Banville, 2020; Les Hutchinson Campos & Maria Novotny, 2018),
- Physical tracking through biometric data (Gates, 2011; Banville, 2023),
- Issues of authorship and copyright (Jessica Reyman, 2013; Timothy Amidon et. al, 2019),
- Assumptions about access (Virginia Eubanks, 2011),
- Classroom implications (Morgan Banville & Jason Sugg, 2021; Estee Beck et al., 2016; Gavin Johnson, 2021),
- Professional workplaces (Mark Andrejevic, 2007); and more.

The following readings build off this investigation and should be viewed as a starting place, but by no means an extensive list.

Assigned Readings[6]:

Amidon, Timothy R.; Hutchinson, Les; Herrington, Tyanna; & Reyman, Jessica. (2019). Copyright, content, and control: Student authorship across educational platforms. *Kairos* 24(1). http://kairos.technorhetoric.net/24.1/topoi/amidon-et-al/index.html.

Banville, Morgan C. (2020). Resisting surveillance: Responding to wearable device privacy policies. *Proceedings of the 38th ACM International Conference on Design of Communication*.

Beauchamp, Toby. (2019). *Going stealth: Transgender politics and U.S. surveillance practices*. Duke University Press.

Beck, Estee; & Hutchinson Campos, Les. (Eds). (2021). *Privacy matters: Conversations about surveillance within and beyond the classroom*. Utah State University Press.

6 This list is certainly not extensive: these are solely suggestions and would shift based on students' interests and goals.

Benjamin, Ruha. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Cambridge, UK; MA: Polity Press.

Browne, Simone. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Clarke, Roger. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498-512.

Dubrofsky, Rachel E.; & Magnet, Shoshana A. (2015). *Feminist surveillance studies*. Durham and London: Duke University Press.

Eubanks, Virginia. (2011). *Digital dead end: Fighting for social justice in the information age*. MIT Press.

Gates, Kelly. (2011). *Finding the face of terror in data. in our biometric future: Facial recognition technology and the culture of surveillance*. NYU Press.

Kafer, Gary; & Grinberg, Daniel. (2019). Editorial: Queer surveillance. *Surveillance & Society* 17(5), 592-601.

Lyon, David. 2022. Reflections on forty years of "surveillance studies." *Surveillance & Society*, 20(4), 353-356. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

Marx, Gary T. (2015). Surveillance studies. *International encyclopedia of the social and behavioral sciences*, 2nd Edition, 733-741.

Moore, Kristen R.; Jones, Natasha; Cundiff, Bailey S.; & Heilig, Leah. (2018). Contested sites of health risks: Using wearable technologies to intervene in racial oppression. *Communication design quarterly review*, 5(4), 52-60.

Noble, Safiya U. (2018). *Algorithms of oppression*. New York: New York University Press.

Young, Sarah. (2023). *Working through surveillance and technical communication*. SUNY Press.

Zuboff, Shoshana. (2019). Age of surveillance capitalism: The fight for a human future at the new frontier of power. *Public Affairs*.

Some of the ideas for course assignments were adapted from Beck, et al. (2021) who wrote about implementing critical digital literacy with undergraduate students. It is important to note that what is included in this article are merely examples. Instructors can, and should, adapt the examples as they see fit, particularly as the readings and assignments relate to students, their positionalities, and their interests. The readings and learning outcomes help prepare students to respond to assignments that center their goals and interests.

Course Assignments[7]:

1. **Keyword Report:** From the reading list, students will select one concept or keyword to further explore. The report must: 1) succinctly define the concept, 2) offer an example of how it could be applied, 3) state how it relates to the course focus on technology, accessibility, and social justice, 4) provide a full citation, and 5) include a multimodal component (an audio description, visual, etc.).

7 Course Assignments 1 and 3 have been adapted from Torin Monahan, 2022.

2. **Case Studies:** Case studies are similar to discussion boards. Each week, students will either have a discussion board or a case study to respond to. Case studies will explore a specific instance of surveillance and/or privacy concerns in the technical/professional workplace. Students will be responsible for utilizing assigned readings, alongside with outside research, to determine the best course of action given the scenario. This project will allow students to identify problems, audiences, and appropriate genres to write in to respond to a case.
3. **Technology Justice Project:** The final project will be a team-based research project, presentation, and reflection. Students will be asked to select a specific social justice concern with technology, formulate research questions, decide upon appropriate research methods to answer their questions, analyze collected data, and compose an accessible final deliverable (i.e., professional report, website, documentary video, podcast, community resources). Sample areas of inquiry might include manufacturing, workplace surveillance, institutional surveillance (CCTV, etc.), algorithmic bias, healthcare inequities, (in)accessible spaces, borders and barriers (airport security, etc.), or other topics that appeal to them.

To assist instructors in introducing some of the listed assignments into their classrooms, I created a mock example of the case study assignment.

Case Study Example[8]

My case study is an example of one of the three major assignments I have designed for the surveillance course. The case contributes to understanding the social justice implications of how different communities are surveilled. Social justice research in technical communication investigates how "communication broadly defined can amplify the agency of oppressed people—those who are materially, socially, politically, and/or economically under-resourced" (Jones, 2016, p. 347). With the shifts in disciplinary focuses in technical communication, students (regardless of major) should center social justice in their approaches to teaching, work, and being in the world.

The Case

This case example is implemented in an upper-division undergraduate technical and professional communication classroom. The prompt for the case asks students to envision four different respective roles in a local company/organization, and how they may communicate in their roles (including specific genres). That is, they may choose any organization in this scenario; regardless of where they choose, there will be an employer, manager, employee, and customer.

In this case, the organization of their choosing is contracted to solve community-based problems; one problem in particular noted a breach of client information. Based on the four different roles, students must respond to the problem:

There is an internal incident where an employee was meeting with a client using

8 This Case Study Example has been piloted successfully in undergraduate upper division writing intensive courses called, "Writing for Business and Industry" and "Business Communication."

Microsoft Teams. The employee did not realize that any messages sent within the chat feature would be viewed by other employees within the company who had access to the channel. It is important that the organization maintains a positive relationship with all clients. Part of this relationship is oftentimes guaranteeing a level of anonymity, as well as confidentiality for client projects and conversations. The company recognizes a need for outlining and communicating best practices for privacy for clients, as well as determining potential risks, consequences, and ethical implications. Your suggested best practices will be read and utilized as internal company policy addressing digital privacy; however, it will also have external application with current and potential clients.

Surveillance and privacy occur within the workplace in different ways—both apparent, and often invisible ways. This example scenario is intended for students to explore best practices of communicating the impacts of surveillance and privacy within the professional workplace, through the perspective of different stakeholders. How do employees communicate about a data breach, versus a manager, for example? This case also demonstrates how instructors and students may approach how technical communicators understand and communicate about biometrics: that is, the information collected such as driver's licenses and passports (among other documents), are personal identifiers of the body and can be distributed. The classroom is one place where instructors and students may analyze the way efficiency is monitored by biometrics—both through how the institution surveils, and the surveillance they may encounter in the workplace. For example, efficiency and biometrics are most often seen in the classroom space with third-party applications, where instructors (and eventually employers) view speed and time as a measure of success. Measures of success, as often determined by "efficiency," manifest through monitoring in learning management systems, or workforce software such as Kronos. They also manifest through remote proctoring such as Respondus and Proctorio, and other third-party software that's introduced within the institution.

Based on this case scenario, students may consider:

- What does efficiency mean to the company, what is considered best performance/practice and by whom?
- How is privacy and surveillance implemented in today's workforce? How are companies defining and enforcing (aka compliance) personal information and biometrics?

Instructors may utilize this activity to spark conversation with students about engaging in digital activism and/or enhancing digital literacy by alerting their peers of how they may be surveilled in the workplace, and also holding employers accountable for how they enact monitoring practices. This case also gives students an opportunity to engage in their own research, exploring questions in their (four) respective roles about privacy leaks:

- What data is at risk?
- Who is most at harm?
- What management plan is in place, and how will clients know that you are in control of the situation?
- What are best practices for maximum efficiency?

- What and which bodies are considered the "norm" that the data is "measured" up against?

This particular classroom case example could lead to a wide range of topics about surveillance and the workplace. Due to recent shifts in surveillance technologies, students and instructors in technical communication must call attention to and explore technological ethics including:

- describing how data and information are collected,
- who has a right to privacy and why,
- and communication exchanges between employer/employee and the public.

Of particular importance and emphasis, students might consider how biometrics as surveillance are utilized in their careers (or future careers). How are biometrics used, perceived, and communicated? How do they (students) view their responsibility (both personal and professional) to communicate about biometrics, and to whom/for whom?

Case Study Implications

By exploring biometric technologies as a case study example of workplace surveillance, students will be able to demonstrate how surveillance is an embodied process, and how they may advocate for individual/user awareness. This classroom scenario is transferable across TPC courses in higher education and institutions. For example, many biometric technologies classify and categorize "like characteristics" often including race and gender identities, which is why it would be much easier to scan a database searching for "like characteristics" to identify, rather than scanning an entire system without categories. Despite the appearance of and communication to consumers of "efficiency," technical communicators should note that this sorting and categorization only serves to contribute to existing forms of biological racialism and sexism, in which "race and gender are imagined as stable biological properties that can be reliably read off the body" (Dubrofsky & Magnet, 2015, p. 15).

As I have written previously (Banville & Sugg, 2021), speaking broadly, the basic tenet of Panopticism is the power of control–control over norms–wherever they may be found. This provides those with power–actual and assumed–to manipulate non-conformity into the authority figures' idea of conformity, thus normalizing the function of surveillance. Employees who surveil can negatively affect trusting relationships between employers and employees. Additionally, surveillance in the work environment places emphasis on achieving success and often puts success over care (Wheeler, 2019). This case scenario seeks to bring awareness to various stakeholders of how society has been slowly turning into a hyper-suspicious assemblage based on the assumed necessity of safety and security, as well as the ways in which biometrics are used to sort and categorize bodies. Technical communicators are well-poised to intervene in language creation and decision-making related to the design of technologies that do not account for, "everyone." Everyone does not benefit from the technology.

Surveillance Pedagogy: Across TPC Programs

Though surveillance is not solely understood as digital, many of the technologies that put bodies on visual display are not new and are rather associated with longstanding forms of oppression. As Agboka and Dorpenyo (2022) note, the social justice turn in TPC has inspired much discussion about programmatic and curricular efforts. At the core of both feminist and social justice methodologies are principles such as access, equity, rights, and participation, all of which facilitate inclusivity, collaboration, diversity, and justice.

As I've argued (Banville, 2023), part of recognizing roles, such as that of a technical communicator, comes from understanding/unpacking actions that are interpreted as privileged. As both instructors and professionals, Rehling argues that professional communication programs prepare students for careers as "writers, editors, document designers, presentation developers, and information managers in technology industries, other businesses, government, and nonprofit organizations" (Kynell-Hunt & Savage, 2004, p. 89). Due to the wide range of careers that students and instructors/administrators are involved in, issues of surveillance must be explored in the classroom space to show how surveillance is not "universally and uniformly applied to all human bodies and, furthermore, monitoring occurs with different degrees of specificity and intention" (Dubrofsky & Magnet, 2015, p. 59). Technical communication instructors are in unique positions to teach students how to analyze and inform audiences of the varying degrees that surveillance is applied to bodies, especially within the professional workplace.

As media scholars danah boyd and Kate Crawford have noted, "Data sets that were once obscure and difficult to manage—and, thus, only of interest to social scientists—are now being aggregated and made easily accessible to anyone who is curious, regardless of their training" (2012, p. 664). Amanda Licastro and Ben Miller (2021) argue that "What's 'big' about big data, then, is not the information itself, but the number of people able to access and interrogate that data" (p. 4). Licastro and Miller (2021) discuss the ways that institutions and writing programs are increasingly using repositories for student data (amongst other data points); however, this may be applied to other structural institutions such as the government or corporations utilizing biometric identification. These institutions, corporations, and governing bodies lack transparency in the process of opting into participation in these systems, which further contributes to ethical concerns about privacy and security. Such topics are apt for consideration when designing technical communication courses, especially since students are stakeholders in these systems (particularly in their future careers) and inform decision-making processes such as the ability to opt out.

Rebecca Dingo (2012) posits, "[Rhetoricians] must examine how rhetorics travel—how rhetorics might be picked up, how rhetorics might become networked with new and different arguments, and how rhetorical meaning might shift and change as a result of these movements" (p. 2). Considering the history and ethical implications of introducing biometrics to different sites of surveillance (different industries students will encounter and/or their specific career paths) is an important aspect

of rhetorical theory and meaning. Rhetoricians and technical communicators alike are well-poised to analyze, intervene in, and reimagine the impact of emerging technologies in various sites. Mais Al-Khateeb (2021) specifically focuses on tracing biometrics, and notes that their "discursive, material, and technological practices" reveal how "such discourses and their promises materialize on bodies of refugees and shape their encounters as 'others and other-others'" (p. 15). Sara Ahmed writes that "others" are those who are marked as different and live within the national body; while "other-others" are those who are different but "may yet be expelled from the national body" (2000, p. 106). This biopolitical control is only one of many ways biometric technologies may be referred to or considered dark or deceptive design, topics of which are commonly discussed in technical and professional communication courses. Biometric technology's introduction through state sanctioned use, often on multiply marginalized people during times of fear and disguised as a necessity for safety, is part of understanding the means through which rhetorics travel. Further, according to Heather Murray (2007), biometric technology is "gauged to the idealized bodies in a given culture, producing as 'abnormal' those who do not correspond to the idealized model…Biometric technology has been made therefore, with a normative notion of 'body' in mind; a culturally constructed notion of embodied identity…" (p. 351). Because of the ways the Panopticon and biometric technologies are designed, the systems give those with power—actual and assumed—the expected norm to measure "non-conformity" to, thus contributing to the everyday form of surveillance.

Introducing students to issues of surveillance within technical and professional communication creates an opportunity to reflect, analyze, and interrogate students' digital literacies. Our identities are inextricably linked and tied to the digital age; digital spaces provide for world-making (Jose Muñoz, 2009). This article contributes to creation of a TPC course including readings and assignments, and focusing on a case scenario to guide students in exploring how surveillance impacts their daily lives. Biometric technologies are one aspect of surveillance that impacts our (as instructors and students) everyday lives. We should discuss with students how and why bodies are impacted by surveillance technologies, especially because technical communicators are, "uniquely poised to function as public intellectuals" (Bowdon, 2004, p. 325). The goals of creating such a course or introducing objectives to curriculum design, are to enact change through intervening in decision-making protocols to advocate and create awareness and transparency of the ways surveillance is heavily intertwined in every aspect of our day-to-day. Due to the rise in digital privacy and surveillance concerns, as well as increasing implementation of emerging technologies in various sectors, higher education courses should address issues involving surveillance as a core learning outcome. This conversation, though situated within the context of higher education courses, can surely extend into secondary education spaces, as well as through workshops for instructors and training materials for technical communicators. After all, surveillance manifests in our everyday life, for everyone.

References

Agboka, Godwin Y; & Dorpenyo, Isidore K. (2022). Curricular efforts in technical communication after the social justice turn. *Journal of Business and Technical Communication*, 36(1), 38-70.

Ahmed, Sara. (2000). *Strange encounters: Embodied others in post-coloniality*. Taylor and Francis.

Al-Khateeb, Mais T. (2020). Toward a rhetoric account of refugee encounters: biometric screening technologies and failed promises of mobility. *Rhetoric Society Quarterly*, 51(1), 15-26. https://doi.org/10.1080/02773945.2020.1841276

Amidon, Timothy R.; Hutchinson, Les; Herrington, Tyanna; & Reyman, Jessica. (2019). Copyright, content, and control: Student authorship across educational platforms. Kairos 24(1). http://kairos.technorhetoric.net/24.1/topoi/amidon-et-al/*index*.html.

Andrejevic, Mark. (2007). *iSpy: Surveillance and Power in the Interactive Era*. University Press of Kansas.

Banville, Morgan C. (2020). Resisting surveillance: Responding to wearable device privacy policies. *Proceedings of the 38th ACM International Conference on Design of Communication*.

Banville, Morgan; & Sugg, Jason. (2021). "Dataveillance" in the classroom: Advocating for transparency and accountability in college classrooms. In *The 39th ACM International Conference on Design of Communication (SIGDOC '21), October 12-14, 2021*, Virtual Event, USA. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3472714.3473617

Banville, Morgan C. (2023). *Am I who I say I am? the illusion of choice: Biometric identification in healthcare* (Order No. 30603350). Available from ProQuest Dissertations & Theses Global. (2830119112). Retrieved from https://www.proquest.com/dissertations-theses/am-i-who-say-illusion-choice-biometric/docview/2830119112/se-2

Morgan C. Banville, Erin Clark, and Kellie Sharp-Hoskins. 2025. Teaching Compliance and Complicity in the Technical Communication Classroom. *Teaching Professional and Technical Communication: A Practicum in a Book*. University of Colorado Press.

Beck, Estee N.; Crow, Angela; McKee, Heidi A.; Reilly, Colleen A.; DeWinter, Jennifer; Vie, Stephanie; Gonzales, Laura; & DeVoss, Dànielle N. (2016). Writing in an age of surveillance, privacy, and net neutrality. *Kairos: A Journal of Rhetoric, Technology, and Pedagogy* 20(2). Retrieved from https://kairos.technorhetoric.net/20.2/topoi/beck-et-al/index.html

Beck, Estee; Goin, M. Ellen; Ho, Andrew; Parks, Alexis; & Rowe, Stephen. (2021). Critical digital literacy as method for teaching tactics of response to online surveillance and privacy erosion. *Computers and Composition*, 61. https://doi.org/10.1016/j.compcom.2021.102654

Benjamin, Ruha. (2019). *Race after technology: Abolitionist tools for the new Jim*

code. Cambridge, UK; MA: Polity Press.

Blake Scott, J.; Longo, Bernadette; & Wills, Katherine V., (Eds.). (2006). *Critical power tools: Technical communication and cultural studies*. Albany: State University of New York Press.

Bowdon, Melody. (2004). Technical communication and the role of the public intellectual: A community HIV-prevention case study. *Technical Communication Quarterly*, 13(3), 325-340

boyd, danah; & Crawford, Kate. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication and Society*, 15(5), 662-79. https://doi.org/10.1080/1369118X.2012.678878.

Brignull, Harry. (2023). Deceptive patterns – user interfaces designed to trick you. *deceptive.design*. Retrieved from https://www.deceptive.design/

Davis, Jessica. (2023, April 23). Most hospital websites routinely transfer patient data via tracking tools. *SC Media: A Cyber Risk Alliance Resource*. https://www.scmagazine.com/analysis/privacy/most-hospital-websites-routinely-transfer-patient-data-via-tracking-tools

Dingo, Rebecca A. (2012). *Networking arguments: Rhetoric, transnational feminism, and public policy writing*. University of Pittsburgh Press.

Dorpenyo, Isidore K. (2019). Risky election, vulnerable technology: Localizing biometric use in elections for the sake of justice. *Technical Communication Quarterly*, 28(4), 361-375. https://doi.org/10.1080/10572252.2019.1610502

Dorpenyo, Isidore K. (2022). Local knowledge as illiterate rhetoric: An antenarrative approach to enacting socially just technical communication. *Journal of Technical Writing and Communication*, 52(3), 291-315. https://doi.org/10.1177/00472816211030199

Dubrofsky, Rachel E.; & Magnet, Shoshana A. (2015). *Feminist surveillance studies*. Durham and London: Duke University Press.

Eubanks, Virginia. (2011). *Digital dead end: Fighting for social justice in the information age*. MIT Press.

Frost, Erin A. (2016). Apparent feminism as a methodology for technical communication and rhetoric. *Journal of Business and Technical Communication*, 30(1), 3–28. https://doi.org/10.1177/1050651915602295

Frost, Erin A.; & Haas, Angela M. (2017). Seeing and knowing the womb: A technofeminist reframing of fetal ultrasound toward a decolonization of our bodies. *Computers and Composition*, 43, 88–105. https://doi.org/10.1016/j.compcom.2016.11.004

Gates, Kelly. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York: New York University Press.

Gilson, Oriana A. (2021). An intersectional feminist rhetorical pedagogy in the technical communication classroom. In Rebecca Walton & Godwin Y. Agboka (Eds.), *Equipping technical communicators for social justice work: Theories, methodologies, and pedagogies* (pp. 178-194). University Press of Colorado. http://www.jstor.org/stable/j.ctv1mjqtfr.13

Hall, Rachel. (2015). Terror and the female grotesque, introducing full-body scanners to U.S. airports. In Rachel E. Dubrofsky & Shoshana A. Magnet (Eds.), *Feminist surveillance studies*, (pp. 127-150). Durham and London: Duke University Press.

hooks, bell. (1994). *Teaching to transgress: Education as the practice of freedom*. New York: Routledge.

Hutchinson, Les; & Novotny, Maria. (2018). Teaching a critical digital literacy of wearables: A feminist surveillance as care pedagogy. *Computers and Composition*, 50, 105-120.

Johnson, Gavin P. (2021). Grades as a technology of surveillance: Normalization, control, and big data in the teaching of writing. In Estee Beck and Les Hutchinson Campos (Eds). *Privacy matters: Conversations about surveillance within and beyond the classroom* (pp. 53-72). Utah State University Press.

Jones, Natasha N. (2016). The technical communicator as advocate: Integrating a social justice approach in technical communication. *Journal of Technical Writing and Communication*, 46(3), 342-361. https://doi.org/10.1177/0047281616639472

Kynell-Hunt, Teresa; & Savage, Gerald. (2004). *Power and legitimacy in technical communication: The historical and contemporary struggle for professional status*. Routledge.

Larson, Selena. (2018, March 18). Beyond passwords: Companies use fingerprints and digital behavior to ID employees. *CNN Business*. https://money.cnn.com/2018/03/18/technology/biometrics-workplace/index.html

Licastro, Amanda; & Miller, Ben. (2021). *Composition and big data*. University of Pittsburgh Press.

Muñoz, Jose E. (2009). *Cruising utopia: The then and there of queer futurity* (sexual cultures, 13). NYU Press.

Murray, Heather. (2007). Monstrous play in negative spaces: Illegible bodies and the cultural construction of biometric technology. *The Communication Review*, 10, 347–365. https://doi.org/10.1080/10714420701715415

Perez, Sarah. (2023, March 23). TikTok CEO says company scans public videos to determine users' ages. *TechCrunch*. https://techcrunch.com/2023/03/23/tiktok-ceo-says-company-scans-public-videos-to-determine-users-ages/

Reilly, Colleen. (2021). Reading risk: Preparing students to develop critical digital literacies and advocate for privacy in digital spaces. *Computers and Composition*, 61. https://doi.org/10.1016/j.compcom.2021.102652

Reissman, Hailey. (2023, February 7). Americans don't understand what companies can do with their personal data—and that's a problem. *TechXplore*. https://techxplore.com/news/2023-02americans-dont-companies-personal-dataand.html

Reyman, Jessica. (2013). User data on the social web: Authorship, agency, and appropriation. *College English*, 75(5), 513–33.

Savytskyi, Taras. (2022, September 22). Research vs vision: The origin story of sony walkman, mini cooper, and the iPhone. *UX Collective*. https://uxdesign.

cc/research-vs-vision-theorigin-story-of-sony-walkman-mini-cooper-and-the-iphone-e5c8623968bc

Seigel, Marika. (2013). *The rhetoric of pregnancy*. University of Chicago Press.

Visa. (2017). *Consumers ready to switch from passwords to biometrics, study shows*. Accessed March 26, 2023, https://usa.visa.com/visa-everywhere/security/how-fingerprint-authentication-works.html

Walton, Rebecca; Moore, Kristen; & Jones, Natasha. (2019). *Technical communication after the social justice turn: Building coalitions for action*. Routledge.

Walton, Rebecca; & Agboka, Godwin. (2021). *Equipping technical communicators for social justice work: Theories, methodologies, and pedagogies*. Utah State University Press.

Wheeler, Annie. (2019). *Taylorism. Key concepts in surveillance studies*. PB Pressbooks.

Woods, Charles; & Wilson, Noah. (2021). The rhetorical implications of data aggregation: Becoming a "dividual" in a data-driven world. *The Journal of Interactive Technology & Pedagogy*, 19. Retrieved from https://jitp.commons.gc.cuny.edu/the-rhetorical-implications-of-data-aggregation-becoming-a-dividual-in-a-data-driven-world/

Author Information

Morgan Banville, Ph.D. is an Assistant Professor of Humanities at Massachusetts Maritime Academy. Her research interests include the intersection of technical communication and surveillance studies, often informed by feminist methodologies. In particular, she examines how biometric technologies are implemented and perceived in medical contexts, and her research was awarded the 2024 CCCC Outstanding Dissertation Award in Technical Communication, the 2021 Outstanding Ph.D. Research Award by the Department of English at ECU and the 2022 and 2023 Graduate Student/NTT Research Award from *Kairos: A Journal of Rhetoric, Technology, and Pedagogy*. You can find her recent work in *Surveillance & Society*, *the Proceedings of the ACM International Conference on Design of Communication* and *IEEE International Professional Communication Conference (ProComm)*, as well as *Programmatic Perspectives*, *Reflections: A Journal of Community-Engaged Writing and Rhetoric*, *constellations: a cultural rhetorics publishing space*, *Journal of Technical Writing and Communication*, and more.