ENGL 3880, Writing for Business and Industry
Case 3: Negotiating Digital Footprints
Instructor: Morgan Banville
Due Date:

Context
You're interning with a local organization who is contracted to solve community-based problems. This project management team that you're on is tasked with deciding best practices for communication both internally and externally for the company.

The team was assigned a new task because of an internal incident where an employee was meeting with a client using Microsoft Teams. The employee did not realize that any messages sent within the chat feature would be seen 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.

Purpose
Surveillance and privacy occur within the workplace in different ways - both apparent, and often invisible ways. This Case #3 is intended for you to explore best practices of communicating the impacts of surveillance and privacy within the professional workplace. For example, you may choose to explore how to navigate systems that provide an illusion of choice - that is, if there is not an option as an employee or client to "opt out" of digital surveillance, what are the ethical implications? Surveillance and privacy concerns affect everyone through surveillance capitalism, the illusion of security, and our right-to-know (Zuboff, 2019 as cited in Reilly, 2021; Kerr, 2009; Youngblood, 2012). You may consider what efficiency means to the company, what is considered best performance/practice and by whom, and how privacy and surveillance is implemented in today's workforce?

Real World Connections/Links
We will discuss a few examples in class; however, it may be useful for you to research data breaches within companies as well as their risk management response to invasion of privacy.

Activities *These are just examples! Others could include a research or recommendation report, or whatever you envision*

Activity 1: Press Release for Future and Current Clientele

- Current clientele received word that there was a leak in privacy, but what does this mean? What data is at risk? 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?
- Write a press release to current, **and** then future clientele demonstrating your ability to respond efficiently to this concern. Ensure that all stakeholders' concerns are articulated and vetted. Remember, your primary audience for the presentation is your client, but your content should reference a basic project plan, whose audience would be public for future clientele.

Activity 2: A PowerPoint Presentation with Voiceover (5 minutes max) to present to your team

- In addition to the content presented in the slides themselves, use the "Voice Over" feature to compose the spoken portion of your presentation. This presentation will require that you quickly build ethos with your team/boss, and that you show your awareness of stakeholders and their varying social positions.
- Your presentation must include the following components:
  - A careful analysis of the rhetorical situation that is created by the case. Your primary audience for this part of the presentation is your boss who will assist in providing feedback for your intended internal company policy.
  - An action plan for facilitating discussion as well as developing an outline for internally documented procedures regarding privacy.
  - *explicit community-based connection; write a policy for the company*

Adopt as you see fit! I suggest putting in parameters: for example, providing evidence/research with x number of sources.

References

Kerr, I., et al. (2009). *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*. Oxford: Oxford University Press.

Reilly, C. (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

Youngblood, S.A. (2012). Balancing the rhetorical tension between right-to-know and security in risk communication: Ambiguity and avoidance. *Journal of Business and Technical Communication, 26*(1), 33-62.