2022

Transforming Privacy Literacy Instruction: From Surveillance Theory to Teaching Practice

Sarah Hartman-Caverly

Alexandria Chisholm

TRANSFORMING PRIVACY LITERACY INSTRUCTION: FROM SURVEILLANCE THEORY TO TEACHING PRACTICE

SARAH HARTMAN-CAVERLY AND ALEXANDRIA CHISHOLM

INTRODUCTION: "PRIVACY LITERACY AND ITS PROBLEMS"

Privacy is a core professional value of library practice. Revelations of state and corporate surveillance, social manipulation, and algorithmic injustice have renewed librarians' interest in privacy instruction (Bulger & Davidson 2018; Harper & Oltmann, 2017; Lamdan, 2019; Leung, Baildon, & Albaugh, 2019; Sander, 2020). The ACRL Framework (2016) articulates privacy-related knowledge practices, and the ALA's Library Bill of Rights (2019) was recently amended to call on libraries to "advocate for, educate about, and protect people's privacy."

Existing models of privacy literacy instruction often focus on frontend privacy settings, data protection, reputation management, and harm reduction (Bawden & Robinson, 2020; Feerrar, 2020; Fortier & Burkell, 2015; Library Freedom, n.d.; Macrina, 2015; Walker, Ferguson, Rowell, Shorish, Bettinger, & Patterson, 2020; Wittek, 2020; Wissinger, 2017). These important, well-intentioned efforts may inadvertently leave participants more vulnerable despite their increased privacy knowledge. Empirical evidence of a privacy control paradox, whereby users with greater perceived control over their informational privacy often end up disclosing more than those with less perceived control, reveals a need to situate privacy literacy efforts in broader contexts of institutionalized privacy harms (Brandimarte, Acquisti, & Loewenstein, 2013).

Hagendorff (2018) outlines four deficiencies in his critique of privacy literacy. First, considering privacy literacy as a form of social capital reveals that existing social inequities result in unequal access to privacy-related learning opportunities. Hagendorff notes that differences in privacy knowledge are observed along lines of education, income, age, race and ethnicity, and gender identity. Such privacy literacy disparities can perpetuate social inequalities through the disparate impacts that institutionalized surveillance imposes on members of vulnerable and marginalized communities (Barocos & Selbst, 2016). Second, Hagendorff questions the premise that users are rational actors with respect to privacy and disclosure, given the realities of persuasive design, digital resignation, algorithmic manipulation, and the persistent myth of the privacy paradox (Kokolakis, 2017; Solove, 2021). Third, Hagendorff critiques the frontend focus of privacy literacy, which contributes to technosolutionism and the control paradox. Finally, Hagendorff observes that user-centric privacy literacy perpetuates responsibilization—a shift of responsibility for privacy governance to the disempowered user, and away from states and corporations. Hagendorff concludes:

> [P]rivacy literacy has to be more than just ticking boxes in the privacy settings. Privacy literacy should comprise the ability to consider involuntary information disclosures by other individuals, to be aware of hidden data collections in devices of the Internet of Things, to know about missing privacy by default settings, and so on. (2018, p. 140)

Informed by Hagendorff's (2018) critique, Hartman-Caverly and Chisholm offer an alternative model for library-led privacy literacy programming. Their theory-informed approach defines privacy literacy as "a suite of knowledge, behaviors, and critical dispositions regarding the information constructs of selfhood, social relationships, and expressive activities" (Hartman-Caverly & Chisholm, 2020, p. 306). The resulting learning experiences are predicated on a positive case for privacy as respect for persons, not just protection for data. The positive case for privacy is depicted in their Six Private I's conceptual framework as seen in Figure 1, which illustrates privacy as zones of protection for one's identity, intellect, bodily and contextual integrity, intimate relationships, freedom of association (interaction) and ability to withdraw into voluntary solitude (isolation) (Hartman-Caverly &

Chisholm, 2020, p. 307). Navigated from the inner core of identity to the outermost sphere of social interaction, these zones of protection are encapsulated by increasingly permeable information boundaries (Cohen, 2019). Privacy literacy supports the individual's awareness of, ability to negotiate, and will to advocate for these boundaries by understanding privacy as a value system rather than a technology (Hartman-Caverly & Chisholm, 2020). The remainder of this paper further explores critical surveillance theories, and related learning activities that enable participants to integrate these theories in the development of privacy literacy.

Figure 1: Hartman-Caverly and Chisholm's Six Private I's Privacy Conceptual Framework

"Calculated Gazes": Algorithmic Injustice in the Data Panopticon

Foucault is broadly cited as the progenitor of critical surveillance theory, and despite renewed allegations about his sexual exploitation of children in Tunisia in the 1960s (Campbell, 2021), it is difficult to discuss the ubiquitous surveillance architecture of today without acknowledging his groundbreaking contributions to its critique. *Discipline and Punish* presents a historical analysis of the transmutation of power from a public spectacle to an internalized and participatory network of "calculated gazes," coercing all members of society in mutual acts of surveillance and social control (Foucault, 1995, p. 177). Foucault recognized Bentham's architectural model for the Panopticon as an effective, efficient, generalizable, and transferable technology for social control, capable of infusing society with an immaterial structure of surveillance architecture (Foucault, 1995).

The panoptic sort represents an early application of Foucauldian surveillance theory to analyze the exploitation of personal data in the information era. Gandy (1993) described the panoptic sort as a "discriminatory technology" involved in the identification, classification, assessment, prediction, and manipulation of human behavior (p. 15). Furthermore, this "totalizing system of social control" creates and perpetuates existing social inequities as it "determines the extent to which individuals will be included or excluded from the flow of information about their environment" (Gandy, 1993, pp. 1, 89). Barocas and Selbst (2016) further demonstrate the disparate impacts of these information asymmetries in their analysis of "digital redlining" (p. 692), which Benjamin (2019) calls "the New Jim Code" (p. 5). She warns that "automated systems… come to make decisions about people's deservedness for all kinds of opportunities" (Benjamin, 2019, p. 10), perpetuating inequalities in a manner that Noble terms "algorithmic oppression" (2019, p. 4).

Privacy literacy learning experiences can support participants in seeing these otherwise invisible "calculated gazes," viewing their own data doubles through a critical lens, and considering their positionality in the panoptic sort. One highly personalized active learning tool is *How Normal Am I?,* an interactive documentary by Tijmen Schep, which offers an engaging introduction to artificial intelligence, biometrics, and implications of modeled data (2020). The user is taken through a series of assessments using a real-time face recognition scan, including predictions for age, gender, beauty score, body mass index, life expectancy, and distractability based on behavioral data. While users receive their various 'scores', Schep contextualizes how this data is measured and how it can be used, or in many cases, misused to make predictions about individuals that can have serious implications on future life opportunities. Schep also highlights several inherent biases to facial recognition technologies, including their propensity to misidentify people of color (Simonite, 2019). An alternate activity that is both less-intrusive and less time-intensive is to ask students to review and respond to Schep's longform infographic, Mathwashing (n.d.). Such learning opportunities can reveal the extent to which users are captive to the pervasive surveillance architecture—and leave them considering the possibility for escape.

"Network of Coercion": Surveillance Capitalism and Digital Resignation

A common critique of privacy work is that privacy is dead, and people no longer care about privacy based on their behavior (Drum, 2013; Marketplace Tech, 2021; Mims, 2018; Popkin, 2010; Sahota, 2020; Sprenger, 1999). While privacy values and behaviors are dynamic and culturally bound, evidence suggests that "privacy is pluralistic - universally recognized and contextually realized" (Hartman-Caverly & Chisholm, 2020, p. 307). The presumption that people no longer care about privacy is borne of the privacy paradox—the observation that people's actual privacy behaviors do not reflect their stated privacy values (Kokolakis, 2017). Recent public polling data challenges the claim that people no longer care about privacy (Auxier, Rainie, Anderson, Perrin, Kumar, & Turner, 2019; Perrin, 2020), and Solove recently declared the privacy paradox a myth arising from the logical fallacy of equating general privacy values with privacy behaviors in a specific context (2021).

The disjuncture between privacy values and behaviors reveals the intentionally clandestine dynamics of the personal data trade. Zuboff warns that technology-mediated social infrastructures are undergirded by surveillance architecture, designed to capture not only data, but the very activities of everyday life. Surveillance capitalism is an emergent mode of profiteering through the reduction of uncertainty by monitoring and manipulating individuals' behavior (2019). The prediction imperative of surveillance capitalism creates a complementary extraction imperative—the necessity to intrude into ever more human activities in order to capture data at scale and at scope (both breadth and depth), and to leverage the resulting information asymmetries in order to control human behavior through actuation (Zuboff, 2019).

Further research demonstrates the futility of even the most privacy literate consumer effectively controlling their personal data. Due to extensive data flows between third party service providers, Noto la Diega and Wharton reasoned that a Google Nest user would need to review approximately one thousand privacy and terms of service agreements in order to make informed data management choices (2016). Another empirical critique of the "notice and choice" privacy paradigm discovered that 74% of study participants bypassed the privacy policy by consenting to a clickwrap license agreement; famously, 93% of participants agreed to 'gotcha' terms of service that entailed signing over one's first-born child to a fictitious social media company (Obar & Oeldorf-Hirsch, 2020). Furthermore, research by Brandimarte, Acquisti and Loewenstein concludes that "'more' control can sometimes lead to 'less' privacy" (2013, p. 345), a phenomenon known as the control paradox.

The information asymmetries and labyrinthine data flows of surveillance capitalism provide no avenue for escape. Explicating what Zuboff calls a "network of coercion" (p. 238) Veronica Barassi observes that "...surveillance capitalism depends on the *systematic coercion of digital participation*, which forces people to give up their personal data to comply with data technologies" (2020, p. 34, emphasis in original). Surveillance architecture dispossesses users of their data, choice, and autonomy by design, such that in Zuboff's stark words, "privacy policies do not matter" (2019, p. 250). As technology increasingly mediates access to human necessities, individuals are left with few meaningful privacy-preserving options, frequently yielding to digital resignation.

Robust privacy literacy instruction should unveil the backend processes of personal data collection and manipulation, and subject them to critical examination—to the limited extent that this is possible. For example, the authors' own original privacy workshop includes a metacognitive activity which enables participants to visit a series of interactive websites (i.e., ClickClickClick, What Every Browser Knows About You, and ad profiles from a variety of social media platforms) and independently explore behavioral surplus data tracking and personal advertisement profiling in real time (Chisholm & Harman-Caverly, 2021b; Moniker, n.d.; Linus, n.d.). Students are then asked to reflect on the experience and anonymously respond to the prompt: "What surprised you about the data that browsers track? Are your ad profiles creepily accurate, or bizarrely inaccurate?" This culminates in a large group discussion, allowing students to volunteer thoughts and instructors to contextualize the experience and answer questions. By giving students hands-on exploration of behavioral data tracking, they are better able to visualize the extent of surveillance of their online activities and can form their own opinions about these practices and their implications. These learning activities inspire participants to consider the degree to which their choices, behaviors, and very consciousness are subject to manipulation by surveillance capitalists.

"An Assault on Awareness": Attention Engineering

Attention is considered a pathway to consciousness, a technique for acquiring knowledge, and a prerequisite to purposeful action (Mole, 2017); thus, it is hardly hyperbolic for Zuboff to assert that "every threat to human autonomy begins with an assault on awareness" (2019, p. 307). The system design factors impacting conscious awareness include attention engineering achieved through persuasive design, in which the user experience is engineered to manipulate people's behaviors and influence their attitudes (Fogg, 2003; Vanden Abeele, 2020; Zuboff, 2019). Informed by Skinnerian behaviorism, persuasive design leverages "captivation metrics"—findings from activity logs interpreted through a psychological lens—to capture user attention and sustain user engagement (Seaver, 2019, p. 429).

Three examples of persuasive design for attention engineering include infinite scroll, choice architecture, and sentiment manipulation. Infinite scroll and autoplay are informed by intermittent conditioning, a technique appropriated from the gambling industry, to induce a state of immersion, time and space distortion, and self-forgetting in the user, in order to increase their engagement and time-on-platform (Montag, Lachmann, Herrlich, & Zweig, 2019; Zuboff, 2019). Infinite scroll and autoplay contribute to doomscrolling behaviors and result in user exposure to increasingly polarized content (DeLeon, 2019; Watercutter, 2020). Choice architecture comprises, in part, the arrangement of system features and deployment of push notifications which subtly condition (or reward) user activity on the platform (Thaler, Sunstein, & Balz, 2012; Zuboff, 2019). Visible engagement metrics, temporal events, algorithmic filter bubbles, and direct sentiment manipulation in users' platform feeds leverage social pressure, peer comparison, fear of missing out (FOMO), and social contagion in order to influence the user base at scale (Kramer, Guillory, & Hancock, 2014). Ultimately, these persuasive design choices construct the user experience to manipulate the user's attention, attitudes, decisions, and behaviors, a process Zuboff describes as actuation (2019).

By recognizing the role of privacy in personal wellbeing, privacy literacy can provide opportunities for conscious consideration of subtle persuasive design choices and their effects on attention. One such example, *The Endless Doomscroller* by Ben Grosser, offers an interactive, endless scroll of generic misfortune to promote reflection on interface design, rhetoric, psychology, and the social architecture of doomscrolling (2021). As users interact with Grosser's digital art installation, they get a sense of the underlying design and intent behind social and digital media platforms' endless newsfeeds. The emotional impact of the experience also reveals how these architectures impact individuals' digital wellbeing. Such learning activities contribute to attention literacy and attention autonomy (Odell, 2019; Rheingold, 2010).

"BE THE FRICTION": NEW APPROACHES TO PRIVACY LITERACY

By shifting the focus of privacy literacy away from front-end platform features and recentering it on people, Hartman-Caverly and Chisholm endeavor to deliver theoretically-grounded, ethics-focused, and person-centered privacy learning experiences. Their Six Private I's privacy conceptual framework facilitates the identification of multifaceted privacy impacts and analysis of otherwise hidden harms (Hartman-Caverly & Chisholm, 2020, p. 307). Highlighting Benjamin's notion of "informed refusal" (2019, p.184), they engage students in active learning, guide students in the application of decision-making frameworks that empower students' self-awareness of their own privacy and disclosure values, and prompt students in informed considerations of privacy benefits, harms, and limits - including the impact of one's own disclosure on others. The authors' privacy literacy work is also informed by attention autonomy (Odell, 2019; Rheingold, 2010) and conscientious connectivity (James, 2014). Their participatory privacy literacy learning experiences enable them to respond to students' expressed needs, interests, and values (Chisholm & Hartman-Caverly, 2020).

The authors' Digital Shred Privacy Literacy Toolkit provides a curated repository of resources to support other educators in developing their own privacy literacy programming (Chisholm & Hartman-Caverly, 2021a). Their emphasis on the positive case for privacy in the human condition makes the resulting privacy literacy learning experiences extensible, generalizable and transferable to a number of curricular and co-curricular contexts, and evergreen in light of technology updates and an evolving regulatory environment. Education alone cannot solve all of the industrial-scale privacy problems that Hagendorff (2018) describes –but it can inspire participants to "be the friction" (Zuboff, 2019, p. 520) in the machine.

REFERENCES

American Library Association [ALA]. (2019, January 19). *Library bill of rights.* http://www.ala.org/advocacy/intfreedom/librarybill

Association of College & Research Libraries [ACRL]. (2016, January 11). *Framework for information literacy for higher education.* http://www.ala.org/acrl/standards/ilframework

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and privacy: Concerned, confused, and feeling lack of control over their personal information.* Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Barassi, V. (2020). *Child data citizen: How tech companies are profiling us from before birth*. MIT Press.

Barocas, S. & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3): 671-732. http://dx.doi.org/10.15779/Z38BG31

Bawden, D. & Robinson, L. (2020). "The dearest of our possessions": Applying Floridi's information privacy concept in models of information behavior and information literacy. *Journal of the Association of Information Science and Technology, 71*(9): 1030-1043. https://doi.org/10.1002/asi.24367

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3): 340–347. https://doi.org/10.1177/1948550612455931

Bulger, M. & Davidson, P. (2018, February). *The promises, challenges, and futures of media literacy*. Data & Society. https://datasociety.net/wp-content/uploads/2018/02/DataAndSociety_Media_Literacy_2018.pdf

Campbell, M. (2021, March 28). French philosopher Michel Foucault 'abused boys in Tunisia.' *The Sunday Times*. https://www.thetimes.co.uk/article/french-philosopher-michel-foucault-abused-boys-in-tunisia-6t5sj7jvw

Chisholm, A. & Hartman-Caverly, S. (2020). *Privacy workshop series.* https://guides.libraries.psu.edu/berks/privacyseries

Chisholm, A. & Hartman-Caverly, S. (2021a). *Digital shred privacy literacy toolkit.* https://sites.psu.edu/digitalshred/

Chisholm, A. & Hartman-Caverly, S. (2021b). *Privacy workshop*. https://guides.libraries.psu.edu/berks/privacy

Cohen, J. E. (2019). Turning privacy inside out. *Theoretical Inquiries in Law*, *20*(1): 1-31. https://doi.org/10.1515/til-2019-0002

DeLeon, H. (2019, April 23). *The ethical and privacy issues of recommendation engines on media platforms*. Towards Data Science. https://towardsdatascience.com/the-ethical-and-privacy-issues-of-recommendation-engines-on-media-platforms-9bea7bcb0abc

Drum, K. (2013, November/December). Privacy is dead. Long live transparency! *Mother Jones*. https://www.motherjones.com/politics/2013/10/future-of-privacy-nsa-snowden/

Feerrar, J. (2020). Supporting digital wellness and wellbeing. In S. Holder & A. Lannon (Eds.), *Student Wellness and Academic Libraries: Case Studies and Activities for Promoting Health and Success* (pp. 169-185). ACRL Press. https://vtechworks.lib.vt.edu/handle/10919/100812

Fogg, B. J. (2003). *Persuasive Technology: Using Computers to Change What We Think and Do*. Morgan Kaufmann.

Fortier, A., & Burkell, J. (2015). Hidden online surveillance: What librarians should know to protect their own privacy and that of their patrons. *Information Technology and Libraries*, *34*(3): 59-72. https://doi.org/10.6017/ital.v34i3.5495

Foucault, M. (1995). *Discipline and punish: The birth of the prison*. (A. Sheridan, Trans.). Vintage Books. (Original work published 1975).

Gandy, O. H. (1993). The panoptic sort: A political economy of personal information. Westview.

Grosser, B. (2021). *The endless doomscroller*. https://endlessdoomscroller.com/

Hagendorff, T. (2018). Privacy literacy and its problems. *Journal of Information Ethics, 27*(2): 127-145.

Harper, L.M. & Oltmann, S.M. (2017). Big data's impact on privacy for librarians and information professionals. *Bulletin of the Association for Information Science and Technology, 43*(4): 19-23. https://doi.org/10.1002/bul2.2017.1720430406

Hartman-Caverly, S. & Chisholm, A. (2020). Privacy literacy instruction practices in academic libraries: Past, present, and possibilities. *IFLA Journal, 46*(4): 305-327. https://doi.org/10.1177/0340035220956804

James, C. (2014). *Disconnected: Youth, new media, and the ethics gap*. MIT Press.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*: 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24): 8788-8790. https://doi.org/10.1073/pnas.1320040111

Lamdan, S. (2019). Librarianship at the crossroads of ICE surveillance. *In the Library with the Lead Pipe*. http://www.inthelibrarywiththeleadpipe.org/2019/ice-surveillance/

Leung, S., Baildon, M., & Albaugh, N. (2019, August 9). *Applying concepts of algorithmic justice to reference, instruction, and collections work*. DSpace@MIT. https://hdl.handle.net/1721.1/122343

Library Freedom. (n.d.). *Library Freedom resources*. https://libraryfreedom.org/resources/

Linus, R. (n.d.). *What every browser knows about you*. https://webkay.robinlinus.com/

Macrina, A. (2015). The Tor browser and intellectual freedom in the digital age. *Reference & User Services Quarterly, 54*(4): 17-20. https://doi.org/10.5860/rusq.54n4.17

Marketplace Tech. (2021, March 15). *One result of one year into the pandemic: Privacy might be dead*. Marketplace. https://www.marketplace.org/shows/marketplace-tech/one-result-of-one-year-into-the-pandemic-privacy-might-be-dead/

Mims, C. (2018, May 6). Privacy is dead. Here's what comes next. *Wall Street Journal*. https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001

Mole, C. (2017). Attention. *Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/entries/attention/

Moniker. (n.d.) *Clickclickclick*. https://clickclickclick.click/

Montag, C., Lachmann, B., Herrlich, M., & Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. *International Journal of Environmental Research and Public Health*, *16*(14), 2612: 1-16. https://doi.org/10.3390/ijerph16142612

Noto La Diega, G. & Walden, I. (2016, February 1). Contracting for the 'Internet of Things': Looking into the Nest. *Queen Mary School of Law Legal Studies,* research paper no. 219/2016. https://ssrn.com/abstract=2725913

Obar, J. A. & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society, 23*(1): 128-147. https://doi.org/10.1080/1369118X.2018.1486870

Odell, J. (2019). *How to do nothing: Resisting the attention economy*. Melville House.

Perrin, A. (2020, April 14). Half of Americans have decided not to use a product or service because of privacy concerns. *Facttank*. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/

Popkin, H. A. S. (2010, January 13). Privacy is dead on Facebook. Get over it. *NBC News*. https://www.nbcnews.com/id/wbna34825225

Rheingold, H. (2010, October 7). Attention, and other 21st-century social media literacies. *EDUCAUSE Review, 45*(5): 14-24. https://er.educause.edu/articles/2010/10/attention-and-other-21stcentury-social-media-literacies

Sahota, N. (2020, October 14). Privacy is dead and most people really don't care. *Forbes*. https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/

Sander, I. (2020). What is critical big data literacy and how can it be implemented? *Internet Policy Review, 9*(2): 1-22. https://doi.org/10.14763/2020.2.1479

Schep, T. (n.d.) *What is mathwashing?* https://www.mathwashing.com/

Schep, T. (2020). *How normal am I?* https://www.tijmenschep.com/how-normal-am-i/

Seaver, N. (2019). Captivating algorithms: Recommender systems as traps. *Journal of Material Culture, 24*(4), 421–436. https://doi.org/10.1177/1359183518820366

Simonite, T. (2019). The best algorithms struggle to recognize black faces equally. *Wired*. https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review, 89*(1): 1-51. http://dx.doi.org/10.2139/ssrn.3536265

Sprenger, P. (1999, January 26). Sun on privacy: 'Get over it.' *Wired*. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2012). Choice architecture. In E. Shafier (Ed.) *The Behavioral Foundations of Public Policy* (pp. 428-439). Princeton University Press. http://dx.doi.org/10.2139/ssrn.2536504

Vanden Abeele, M. M. P. (2020). Digital wellbeing as a dynamic construct. *Communication Theory,* 1-24. https://doi.org/10.1093/ct/qtaa024

Walker, P., Ferguson, J., Rowell, C. J., Shorish, Y., Bettinger, E., & Patterson, B. (2020). *Digital privacy instruction curriculum*. https://doi.org/10.17605/OSF.IO/SEBHF

Watercutter, A. (2020, June 25). Doomscrolling is slowly eroding your mental health. *Wired*. https://www.wired.com/story/stop-doomscrolling/

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy, 11*(2): 378-389. https://doi.org/10.15760/comminfolit.2017.11.2.9

Wittek, L. (2020). Incorporating online privacy skills into one-shot sessions. *Library Hi Tech News, 37*(4): 15-17. https://doi.org/10.1108/LHTN-01-2020-0004

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Hachette Book Group.

Images for Tables and Figures (Editor will put in body of the text later)

Figure 1