Why Privacy and Why Now?

DENISE FITZGERALD QUINTEL AND AMY YORK

In many ways, we are all still reeling from 2020. Caregivers, parents, children, educators, and virtually everyone took on numerous roles and responsibilities while coping with losses, grief, and trauma that we all seemed to share collectively. There was a consistent need to connect and find community when the world seemed to shut down around us, with so many navigating spaces that seemed impossible to pass.

Unsurprisingly, the start of the COVID-19 pandemic altered the educational landscape on a tremendous scale. The rush to emergency remote learning was one of the most significant challenges that educators, parents, and students faced, and it is something that still impacts us. Even though schools have returned to in-person classes, online platforms hastily adopted in 2020 remain used as course management, communication, or content delivery tools. Privacy issues related to education are not new, but the sudden shift to online learning brought these concerns into sharp focus for many parents, educators, administrators, and researchers.

The objective of this book is to reflect on the unintended breaches of privacy, safety, and security that occurred during 2020 and how those events continue to shape online educational spaces. Within these chapters, contributors examine their own teaching experiences and propose solutions for more responsible use of online platforms and tools. This book documents how educational institutions approach privacy. It describes initiatives implemented in response to online learning and contributes to the growing discussion of how privacy and surveillance impact our users, especially students from our most vulnerable populations.

In 2020, Pew Research presented survey results illustrating a growing problem with how private companies collect our data. In the prior year, three-quarters of Americans (72%) believed that private companies utilized almost all their data, and nearly half (47%) believed the government was also surveilling their data (Auxier et al., 2019). The COVID-19 pandemic response created more concerns as government and private companies used personal devices for tracking individuals testing positive for the virus. However, while most Americans feel uneasy about their data being collected, many also think that privacy protection concepts are too complex to understand or implement on our own (Auxier, 2019). As editors, we could not anticipate the sheer number of privacy issues that would continue to impact news stories while compiling this book between 2021 and 2022.

Although there have been reports on the data collection business for a while (Valentin-DeVries et al., 2018), we have been on high alert for location tracking and collecting personal health data this past year. Most notably, after the Supreme Court overturned Roe V. Wade, many people deleted menstrual cycle-tracking apps from their phones (Kwong et al., 2022). Still, those actions sparked more discussion into how many ways our data is collected and identifiable whenever we use a smartphone, website, or Google search (Hill, 2022). Reporters investigated data brokers and demonstrated the incredible ease and surprisingly low cost involved with purchasing and then deanonymizing aggregate data (Cox, 2022).

There were legal wins against proctoring software in the education world, declaring room scans unconstitutional (Bowman, 2022). More reports surfaced on how online proctoring poses significant problems for users with disabilities (Brown, 2022). Additionally, student activity monitoring software, which became more widely used during the shift to online learning, is still being used by institutions at a global level despite numerous red flags (CDT, 2021; Singer, 2022). Even the youngest children and their families are at risk, as we are now seeing reports on how daycare apps are rife with security and data issues (Gruber et al., 2022; Hancock, 2022).

 https://doi.org/10.56638/mtopb00123

We saw library service providers purchased by data analytics companies for billions (USD), moving away from traditional publishing companies and finding new ways to monetize data points in addition to scholarly research (Lamdan et al., 2021). In some cases, we saw library vendors engage in partnerships with government agencies, granting access to the personal data of millions (Coldeway, 2022; Lamdan, 2019; Lui, 2022). We saw numerous data breaches in school districts and higher education institutions (Bamforth, 2022; Freed, 2022; Johnson, 2022). Even if these schools paid the ransom, there would be no guarantee that these institutions would recover their data (Klein, 2022; Mahendru, 2022; Page, 2022; Singer, 2022). Privacy is far from a new or novel concept in education, but as more of these stories bubbled to the surface, it was clear that concerns were valid and piqued public interest.

While many families balked at the surveillance features in school-provided technology (Ceres, 2022), some chose to double down on surveillance measures for their children in 2020. We witnessed multiple states enact legislation to censor library materials (Iowa 2176; Oklahoma SB1142; Indiana SB17; Idaho HB666; Tennessee HB/SB1944). At a local level, even school boards censored materials (Mangrum, 2021). In response to legislation, we watched a company, through their technology, attempt to give parents unfettered access to their child's library history without the consent of their children. Included in that technology would also be an effortless way for parents to restrict materials, such as anything tagged for LGBTQ content (Ellis, 2022). Some may argue that libraries should use surveillance measures for protection. Nevertheless, with surveillance technologies, it is essential to look closely at how companies and their parent companies engage in business (Gallagher, 2020; Krapiva & Micek, 2020).

As library professionals, we want to point out that privacy is a core value of our profession. Any attempt to censor, restrict, monitor, or suppress the free flow of ideas is antithetical to intellectual freedom. Groups who push for censorship in libraries to "protect" children directly oppose what safe spaces for learning, creating, and self-expression look like for all children.

> *Privacy is essential to the exercise of free speech, free thought, and free association. Lack of privacy and confidentiality chills users' choices, thereby suppressing access to ideas. The possibility of surveillance, whether direct or through access to records of speech, research, and exploration, undermines a democratic society.*
> – Privacy: An Interpretation of the Library Bill of Rights

***

The chapters collected in this book describe a wide array of privacy issues in online and remote learning environments. Our contributors go beyond the practical takeaways for keeping information and data safe. We see how educators, librarians, and administrators share an underlying motivation to protect their students while safeguarding students' autonomy. The authors capture the frantic energy many educators experienced as we shifted to emergency remote learning and how it shaped and continues to influence these online spaces. Their experiences are as varied as their online spaces, as we hear from writing centers, out-of-school elementary programs, libraries, middle schools, and universities.

We have organized the book into different sections, each attempting to answer an overarching question. Section I

provides an overview of what institutions currently do to address privacy concerns. Contributors share how to build collaborative, safe learning policies and reveal the shortcomings of the Family Educational Rights and Privacy Act (FERPA). One author shares her approach to collaborative policy building, where all voices and viewpoints will have a seat at the table to craft ways to address privacy issues. Another addresses online privacy culture through the lens of an academic librarian, which involves increasing accountability at a system level rather than at the individual.

Section II looks closely at how we can protect our students and ourselves as educators. Authors bring the voices of transgender, non-binary, and gender-diverse students to the discussion and ask readers to listen to how we could improve their online experiences. Authors provide ways to help ensure instructor safety as lines between personal and professional life often blur during remote instruction. The chapters cover doxing, online bullying, and library-induced anxiety.

Section III examines how others have built or transformed their online pedagogy to incorporate privacy and safety concerns. We ask readers to consider what privacy looks like for marginalized groups and at-risk students and how we can improve the care for our students and ourselves. We hear about building authentic connections with our students while protecting their private lives. We learn how a trauma-informed pedagogy can help students and how privacy included in universal design learning benefits everyone.

Lastly, in section IV, the authors provide several tools and resources that one can implement into their online instructional spaces. The authors discuss privacy tools ranging from artificial intelligence (AI) methods to proctoring alternatives and best practices for storing data. Many authors share valuable privacy-focused resources and tools that an educator can consider, ranging from beginner to expert-level experience for implementation.

***

While the idea for this book came from the experiences that we, as co-editors, had as parents, librarians, caregivers, and on-call teachers during the early stages of the COVID-19 pandemic, our original book title solely referenced remote learning. As readers will see in the following chapters, even though initial experiences occurred during emergency remote teaching (ERT), the lessons and resources shared go beyond any single environment and can inform several types of instruction and educational backgrounds. Like the legal realm, privacy in educational settings is a concept that cannot be defined as one thing but contains many ideas and definitions (Hertzog, 2021).

When we sent out the initial call for chapters, we were unsure how receptive scholars, practitioners, and educators would be.

The response was stunning.

While this book will not have all the answers to your questions, it provides a great starting point for those interested in addressing privacy, safety, and security concerns in their own online and remote educational environments.

> "*All of this to say that:*
> *You deserve safety & agency*
> *You deserve more & better*
> *Then what is offered.*"
> – Library Freedom Project FINSTA Project, 2020

References

American Library Association. (2021, October 20). *Core values*. Advocacy, Legislation & Issues. https://www.ala.org/advocacy/privacy/values

Auxier, B. (2020, August 27). *How Americans see digital privacy issues amid the COVID-19 outbreak*. Pew Research Center. https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/

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/

Bamforth, E. (2022, May 2). *After ransomware, Austin Peay moves ahead with finals*. EdScoop. https://edscoop.com/austin-peay-state-university-ransomware-finals-petition/

Bowman, E. (2022, August 26). *Scanning students' rooms during remote tests is unconstitutional, judge rules*. NPR. https://www.npr.org/2022/08/25/1119337956/test-proctoring-room-scans-unconstitutional-cleveland-state-university

Brown, L. X. Z. (2021, June 23). *How automated test proctoring software discriminates against disabled students*. Center for Democracy and Technology. https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/

Ceres, P. (2022, October 10). *How to protect yourself if your school uses surveillance tech*. Wired. https://www.wired.com/story/how-to-protect-yourself-school-surveillance-tech-privacy/

Cox, J. (2022, May 3). *Data broker is selling location data of people who visit abortion clinics*. VICE. https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood

Coldewey, D. (2022, June 9). *Records show ICE uses LexisNexis to check millions, far more than previously thought*. TechCrunch. https://techcrunch.com/2022/06/09/records-show-ice-uses-lexisnexis-to-check-millions-far-more-than-previously-thought/

Ellis, D. (2022, April 4). *Technology for parent monitoring of Student Library use is being developed by Follett: This Week's book Censorship News April 1, 2022*. Book Riot. https://bookriot.com/book-censorship-news-april-1-2022/

Freed, B. (2022, January 14). *Albuquerque, New Mexico, schools closed after cyberattack*. State Scoop. https://statescoop.com/albuquerque-new-mexico-schools-closed-after-cyberattack/

Gallagher, R. (2020, August 28). *Belarusian officials shut down internet with technology made by U.S. firm*. Bloomberg.com. https://www.bloomberg.com/news/articles/2020-08-28/belarusian-officials-shut-down-internet-with-technology-made-by-u-s-firm?leadSource=uverify+wall

Gallagher, R. (2021, January 26). *Private equity firm Francisco Partners profits from surveillance, censorship*. Bloomberg.com. https://www.bloomberg.com/news/features/2021-01-26/private-equity-firm-francisco-partners-profits-from-surveillance-censorship

Grant-Chapman, H., Laird, E., & Venzke, C. (2022, May 19). *Student activity monitoring software: Research insights and recommendations*. Center for Democracy and Technology. https://cdt.org/insights/student-activity-monitoring-software-research-insights-and-recommendations/

Gruber, M., Höfig, C., Golla, M., Urban, T., & Große-Kampmann, M. (2022). "We may share the number of diaper changes": A privacy and security analysis of Mobile Child Care Applications. *Proceedings on Privacy Enhancing Technologies*, 2022(3), 394–414. https://doi.org/10.56553/popets-2022-0078

Hancock, A. (2022, June 27). *Daycare apps are dangerously insecure*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2022/06/daycare-apps-are-dangerously-insecure

Hartzog, W. (2021). What is privacy? That's the wrong question. *The University of Chicago Law Review*, 88(7), 1677–1688. https://www.jstor.org/stable/27073959

Hill, K. (2022, July 11). Deleting your period tracker won't protect you. *New York Times*. https://www.nytimes.com/2022/06/30/technology/period-tracker-privacy-abortion.html

House Bill 666. (2022, July 1). 66th Legislature of the State of Idaho. https://legislature.idaho.gov/sessioninfo/2022/legislation/H0666/

House Bill 1944 (2022, March 30). 112th General Assembly of the State of Tennessee. https://www.capitol.tn.gov/Bills/112/Bill/HB1944.pdf

House File 2176. (2022, February 1). 89th General Assembly of the State of Iowa. https://www.legis.iowa.gov/legislation/BillBook?ga=89&ba=HF2176

Klein, A. (2022, March 31). *What schools can learn from the biggest cyberattack ever on a single district*. Education Week. https://www.edweek.org/technology/what-schools-can-learn-from-the-biggest-cyberattack-ever-on-a-single-district/2022/03

Krapiva, N., & Micek, P. (2020, September 4). *Francisco Partners-owned Sandvine profits from shutdowns and oppression in Belarus*. Access Now. https://www.accessnow.org/francisco-partners-owned-sandvine-profits-from-shutdowns-and-oppression-in-belarus/

Kwong, E., Ramirez, R., & Cirino, M. (2022, January 18). *When tracking your period lets companies track you*. NPR. https://www.npr.org/2021/12/29/1068930998/when-tracking-your-period-lets-companies-track-you

Lamdan, S. (2019, November 13). *Librarianship at the crossroads of ICE Surveillance*. In the Library with the Lead Pipe. https://www.inthelibrarywiththeleadpipe.org/2019/ice-surveillance/

Lamdan, S., Montoya, R., Swauger, S., & Halperin, J. R. (2021, December). *The conquest of ProQuest and Knowledge Unlatched: How recent mergers are bad for research and the public*. Invest in Open Infrastructure. https://investinopen.org/blog/the-conquest-of-proquest-and-knowledge-unlatched-how-recent-mergers-are-bad-for-research-and-the-public/

Library Freedom Project. (2021, April). *The FINSTA project: What educational tech knows*. Library Freedom Project. https://libraryfreedom.org/finsta-project/

Lui, Y. (2022). LexisNexis and I.C.E.: An examination of LexisNexis's human rights responsibilities. *Journal of International Law and Politics*, 54(23), 69–84. https://www.nyujilp.org/lexisnexis-and-i-c-e-an-examination-of-lexisnexiss-human-rights-responsibilities/

Mahendru, P. (2022, July 12). *The state of Ransomware in education 2022*. Sophos News. https://news.sophos.com/en-us/2022/07/12/the-state-of-ransomware-in-education-2022/

Mangrum, M. (2021, October 21). Tennessee librarians speak out against Chattanooga school board member's attempt to

ban books. *The Tennessean*. https://www.tennessean.com/story/news/education/2021/10/21/tennessee-librarians-speak-out-against-chattanooga-school-board-members-attempt-have-books-banned-sc/6119874001/

Page, C. (2021, November 22). *US education software company exposed personal data of 1.2M students*. TechCrunch. https://techcrunch.com/2021/11/22/smarterselect-exposed-millions-student-data/

Senate Bill 17. (2022, January 28). 122nd General Assembly of the State of Indiana. https://iga.in.gov/documents/221c1669

Senate Bill 1142. (2021, December 16). 58th Legislature of the State of Oklahoma. http://www.oklegislature.gov/BillInfo.aspx?Bill=SB1142&Session=2200

Senate Bill 1944. (2022, April 6). General Assembly of the State of Tennessee. https://www.capitol.tn.gov/Bills/112/Bill/SB1944.pdf

Singer, N. (2022, July 31). A cyberattack illuminates the shaky state of student privacy. *New York Times*. https://www.nytimes.com/2022/07/31/business/student-privacy-illuminate-hack.html

Valentin-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your apps know where you've been and can't keep a secret. *New York Times*. https://ezproxy.mtsu.edu/login?url=https://www.proquest.com/newspapers/your-apps-know-where-youve-been-cant-keep-secret/docview/2153542863/se-2