ASPEN TECH POLICY HUB

POLICY

Strengthening Student Data Protection in New Mexico

ALIJA BLACKWELL

EXECUTIVE SUMMARY

The New Mexico Public Education Department (NMPED) should mandate that school districts include a student data protection agreement in educational technology vendor contracts to create safer virtual learning environments for students statewide. To ensure that school districts and educational technology vendors comply with this agreement, the NMPED should establish a Student Data Protection Office funded by the US Department of Education's Elementary and Secondary School Emergency Relief (ESSER) Fund to oversee the implementation, training, and evaluation of student data protections across school districts.

BACKGROUND

New Mexico's primary educational technology vendor, Google's G Suite for Education on school-issued Chromebooks, has a record of violating student data protections. In 2018 and 2020, the New Mexico attorney general sued Google for collecting children's data without parental consent.[1] In 2019, the Federal Trade Commission issued the largest civil penalty in history to Google for violating the Children's Online Privacy Protection Act by collecting children's data without parental consent via YouTube, an application widely accessed by students.[2] In a 2013 lawsuit related to student data privacy, Google officials confirmed that they scan and index emails from student accounts for targeted advertising, among other purposes.[3]

Case Studies of the Harms of Student Data Mining and Profiling

Student data profiling by educational technology platforms disproportionately affects students of color and students from low-

income communities. Students of color make up over 80 percent of the enrollment in New Mexico public schools, and almost a third of all students are from low-income households.[4] Student data profiling has harmful consequences, such as limiting access to opportunities for economic mobility, growing the preschool to prison pipeline, and increasing the risk of sensitive data being breached.

- **Economic Mobility.** The threat of student data profiles being used to determine access to opportunities for economic mobility into adulthood is imminent. Between school vendors engaging in third-party student data sharing and cases of the illegal sale of student data, there is an increased potential for student data to be used for unintended purposes, including hiring decisions, higher education admissions, and insurance rates.[5]

- **Preschool to Prison Pipeline.** The student data aggregated across school-issued devices on school-managed internet have been shared with third parties to target students based on social identity and past behavior. For example, the Pasco County School District in Florida shared student data with local law enforcement, without seeking parental consent or notifying parents, to identify and surveil at-risk youth flagged by monitoring software as having the potential to commit crimes.[6] The factors used to flag students included personally identifiable information and education records such as class attendance, school discipline data, and previous interactions with law enforcement. The US Department of Education is investigating the school district to determine whether it violated federal student privacy laws.

- **Data Breaches.** The practice of student data mining without comprehensive cybersecurity infrastructure across schools and edtech vendors increases the risk of data breaches. As schools and their vendors have increasingly been targeted by ransomware attacks, the risk of identity theft and financial losses through the widespread collection, retention, and sharing of student data has strengthened.[7] For example, school districts across New Mexico have experienced data breaches over the past few years.[8] Most recently, the Albuquerque Public School District, the largest public school district in New

Mexico, closed all 114 schools because of a ransomware attack that locked school administrators and personnel out of their systems from January 13, 2022, through the Martin Luther King Jr. holiday weekend.[9] The personally identifiable information of over 75,000 students and school community members was breached, resulting in a $300,000 investigation.[10]

RECOMMENDATION

Google's history of profiling student data must be met with more proactive and comprehensive student data protection practices to ensure safe virtual learning environments for future generations. New Mexico has the opportunity to be a national leader in modeling comprehensive statewide student data protections. By implementing a student data protection agreement as a uniform standard, the NMPED can protect over 350,000 students currently left vulnerable to extractive data mining practices in online learning environments mediated by educational technology platforms.

Such an agreement should be modeled on the Student Data Privacy Consortium's (SDPC) National Data Privacy Agreement, but with important modifications. (See sample Student Data Privacy Agreement.) Implementing such an agreement will have several benefits for the NMPED:

- **Uniform standards across school districts would streamline data protection monitoring and compliance to advance equitable learning environments.** The student data protection agreement would create more efficient procedures to ensure that schools and vendors are meeting security and privacy standards. Uniform standards would also support the NMPED in meeting its goal of creating more equitable learning environments by limiting student data profiling.[11]
- **Data protection agreements would proactively ensure student safety in digital learning environments to prevent financial and legal losses.** Establishing such an agreement across school districts would bridge the gaps in current government regulations and vendor policies related to students' digital rights. By setting a common understanding of security and

privacy standards for both vendors and schools, the NMPED would help identify and mitigate the risks of student data sharing to better protect education data from being collected, distributed, or used for unintended purposes.

To support future-ready technology leaders in creating safe, student-centered learning environments, the NMPED should establish the Office of Student Data Protection to oversee training, monitoring, and compliance with the agreement. Creating such an office will propel the NMPED toward being a national leader in the following ways:

- **A centralized Office of Student Data Protection would enable future-ready technology leaders in creating safe, student-centered learning environments with ongoing training, monitoring, and enforcement.** The Student Data Protection Office and student data protection agreement would fulfill NMPED's effort with the Alliance for Excellent Education's Future Ready Schools effort to ensure data safety, security, and privacy. The agreement would "create and enforce mechanisms that ensure student data privacy, while educating staff members on the various laws, policies, and expectations around data privacy and security."[12]

- **The office would advance statewide education cybersecurity practices to reach national and state goals to secure the digital learning infrastructure.** As NMPED and the state Office of Broadband Access and Expansion continue broadband expansion and digital literacy efforts, establishing a central coordinating office would position the state for a secure online ecosystem.[13] Further, this would support the landmark *Yazzie/Martinez v. State of New Mexico* case's motion to invest in statewide school technology infrastructure that is essential to a "constitutionally sufficient education."[14] Additionally, the office would support the proposed House Bill 122 school cybersecurity program in implementing data protections for the statewide educational technology infrastructure.

The implementation of the Student Data Protection Office and data protection agreement should be resourced by $20 million to

$25 million of the $979,056,256 allocated by the US Department of Education's Elementary and Secondary School Emergency Relief (ESSER) Fund that is eligible to be spent by September 30, 2024.[15]

For more information on this proposal, please see the sample Student Data Protection Agreement and an operational plan to establish the Student Data Protection Office.

ENDNOTES

1 New Mexico Office of the Attorney General, "AG Balderas Announces Lawsuit Against Tech Giants Who Illegally Monitor Child Location, Personal Data: Google, Twitter, Tiny Lab among Companies Who Unlawfully Market to Children," news release, September 12, 2018, https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Announces_Lawsuit_Against_Tech_Giants_Who_Illegally_Monitor_Child_Location__Personal_Data_1.pdf; "Attorney General Balderas Sues Google for Illegally Collecting Personal Data of New Mexican School Children," news release, February 20, 2020, https://www.nmag.gov/uploads/PressRelease/48737699ae174b30ac51a7eb286e661f/AG_Balderas_Sues_Google_for_Illegally_Collecting_Personal_Data_of_New_Mexican_School_Children.pdf.

2 Federal Trade Commission, "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law," news release, September 4, 2019, https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations; Federal Trade Commission, "Dissenting Statement of Commissioner Rohit Chopra in the Matter of Google LLC and YouTube LLC," news release, September 4, 2019, https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf.

3 Benjamin Herold, "Google Under Fire for Data-Mining Student Email Messages," *Education Week*, March 13, 2014, https://www.edweek.org/policy-politics/google-under-fire-for-data-mining-student-email-messages/2014/03?cmp=ptnr-hp.

4 The Annie E. Casey Foundation, "2020 Kids Count Data Book: 2020 State Trends in Child Well-Being," June 22, 2020, https://www.aecf.org/resources/2020-kids-count-data-book.

5 Barbara Kurshan, "The Elephant in the Room with EdTech Data Privacy," *Forbes*, June 22, 2017, https://www.forbes.com/sites/barbarakurshan/2017/06/22/the-elephant-in-the-room-with-edtech-data-privacy/?sh=5f0f81c357a5.

6 Legal Defense Fund, "New Coalition Formed to End Pasco County's Predictive Policing Program," April 26, 2021, https://www.naacpldf.org/press-release/new-coalition-formed-to-end-pasco-countys-predictive-policing-program/; Associated Press, "Federal Investigators to Probe Florida School Policing Plan," April 19, 2021, https://apnews.com/article/lawsuits-florida-tampa-crime-b4525f17eb65fb596633950fc640bd54.

7 Children's Commissioner for England, "Who Knows What About Me? A Children's Commissioner Report into the Collection and Sharing of Children's Data," November 2018, https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/cco-who-knows-what-about-me.pdf.

8 Rachel Knapp, "Albuquerque Public Schools Renews Contract with Cyber Protection Service," KRQE, updated January 21, 2020, https://www.krqe.com/news/education/albuquerque-public-schools-renews-contract-with-cyber-protection-service/.

9 Albuquerque Public Schools, "APS Resolves Ransomware Attack," January 19, 2022, https://www.aps.edu/news/news-from-2021-2022/aps-resolves-ransomware-attack.

10 Rick Nathanson, "Ransomware Attack on APS Is Now Resolved," *Albuquerque Journal*, updated January 19, 2022, https://www.abqjournal.com/2462462/ransomware-attack-on-aps-is-now-resolved-ex-fbi-advises-school-offic.html.

11 Education Resource Strategies, "Leveraging Federal Stimulus Funds for Equity-Focused Recovery and Redesign," May 27, 2021, https://www.erstrategies.org/tap/ESSER_for_equity.

12 Alliance for Excellent Education, "Future-Ready Schools," September 2018, https://webnew.ped.state.nm.us/wp-content/uploads/2018/09/Tech_leader_flyer6.16.17.pdf.

ASPEN TECH POLICY HUB

POLICY

13 New Mexico Department of Information Technology, "State of New Mexico Broadband Strategic Plan and Rural Broadband Assessment," June 2020, https://www.doit.state.nm.us/broadband/reports/nmbbp_strategic20200616Rev2Final.pdf.

14 Transform Education New Mexico, "Platform for Transformation," February 2021, https://transformeducationnm.org/our-platform/.

15 US Office of Elementary and Secondary Education, "American Rescue Plan Elementary and Secondary School Emergency Relief Fund," March 2021, https://oese.ed.gov/files/2021/03/FINAL_ARP-ESSER-Methodology-and-Table.pdf.

ABOUT THE HUB

The Aspen Tech Policy Hub is a Bay Area policy incubator, training a new generation of tech policy entrepreneurs. We take tech experts, teach them the policy process, and support them in creating outside-the-box solutions to society's problems..

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

THE ASPEN INSTITUTE