International Journal of Communication 16(2022), 767–788 1932–8036/20220005

Data Privacy Literacy as a Subversive Instrument to Datafication

VELISLAVA HILLMAN
London School of Economics and Political Science, UK

To learn about the risks from their data privacy loss, children need look no further. Digitalized education has propelled constant data extraction and—hypocritically—a *privacy standard* that contrasts with data privacy literacy efforts that policy and academics promote. If *School* allows data extraction from its ubiquitous digitalization, what do children learn about their privacy? Moreover, is edtech's commercial project for School a form of hidden pedagogy for oppression creating and reinforcing this hypocrisy? These questions emerge as I critically examine data privacy conceptually and observe School's data privacy practices in contrast with proposals for teaching data privacy literacy. For such teachings to succeed, School must unveil the hypocrisy of data practices that are enabled as every educational process becomes digitalized and, through copartnership with students, commit to recreating privacy preservation independent of corporate influence reality.

Keywords: data privacy, dataveillance, children, edtech, data privacy literacy

Datafication, seen as turning social action into online quantified data to allow for real-time tracking and predictive analytics (Mayer-Schönberger & Cukier, 2013), promises in education similar results—tracking of real-time student behavior in digitally mediated learning environments for predicting, adapting, and "personalizing" the educational experience (Mayer-Schönberger & Cukier, 2013). To *School*, capitalized as a way of generalizing public education and also any educational institution that performs certain functions for which it is held accountable, datafication becomes the means to improving these functions and enabling some kind of accountability (Mandinach & Schildkamp, 2021).

The exploitative nature of education technology businesses (edtech) whose products and services drive datafication advance their position in School in response to accountability demands; as the means to progress within a neoliberal paradigm (Zuboff, 2019); as an investor that "banks" its resources in School, promising children employable futures (Eisenstadt, 2021); and as a savior that delivers tactical generosity by reimagining education through technologies (Fullan, Quinn, Drummy, & Gardner, 2020; United Nations Educational, Scientific and Cultural Organization [UNESCO], 2020).

Datafication in education, however, has also intensified the debate surrounding the risks of privacy loss through surveillance or "dataveillance" (van Dijck, 2014, p. 198), enabling behavior control (Andrejevic

Velislava Hillman: v.hillman@lse.ac.uk
Date submitted: 2021-03-25

& Selwyn, 2020), diminishing personal freedoms and rights (Lupton & Williamson, 2017), and creating information asymmetries (Brunton & Nissenbaum, 2015). More broadly, datafication is also seen as a form of colonizing populations as the captured personal information can enable their control (Couldry & Mejas, 2019). While the narratives of personal data anonymization and deidentification continue to hold false promises (Cavoukian & Castro, 2014), these are far from able to safeguard individual privacy (Solove & Schwartz, 2020). Meanwhile, such risks have little effect over the decision making of governments globally (Bozkurt et al., 2020; United Kingdom Department for Education [DfE], 2020; United States Department of Education [DoE], 2017) as they let industries that enable datafication into public education without regulatory or licensing regimes and clear procurement standards (Day, 2021).

Against some of these risks emanating from datafication, growing scholarship has come to propose data and privacy literacy curricula. Some advocate online privacy literacy to support self-data protection and self-determination (Masur, 2020). Others have designed a personal data literacies framework (Pangrazio & Selwyn, 2020) and models for social data and privacy (Fontichiaro & Oehrli, 2016). Still others suggest that School should teach data and privacy literacy as a skill (Stoilova, Livingstone, & Nandagiri, 2021). Yet a sort of "teach but not practice" hypocrisy emanates when, in reality, School and policy makers allow constant student data exchanges with thousands of edtech. Moreover, such proposals will be rendered ineffective as edtech advance further into education. To support this argument, I use two angles of analysis. The first adopts from Bourdieu's (re)production in education (Bourdieu & Passeron, 1977/2000) and sees edtech beginning to occupy a certain *pedagogic power* through their products, which increasingly come to mediate educational processes. This pedagogic power accumulates through *pedagogic action* and *pedagogic work,* which are expressed by the ability of edtech to extract student data for algorithmic decision making. The pedagogic action and pedagogic work legitimize the datafication processes and raise edtech as *pedagogic authority*. As such, edtech can have the capacity to legitimize their own pedagogic dominance and therefore influence the (re)production of education. Crucially, it is on School's grounds that this new pedagogic authority emerges. As such, School either does not recognize or does not present an honest account of the power dynamics at play as edtech become ever more central to education by mediating their processes. The theory of symbolic violence (Bourdieu & Passeron, 1977/2000) lends itself to parallel that the edtech data-dependent products become the delegation which establish[es] the pedagogic action, in addition to a delimitation of the content inculcated, a definition of the mode of inculcation (the legitimate mode of inculcation) and of the length of inculcation (the legitimate training period), which define the degree of completion of pedagogic work considered necessary and sufficient to produce the accomplished form of the habitus, i.e., the degree of cultural attainment (the degree of legitimate competence) by which a group or class recognizes the accomplished man (Bourdieu & Passeron, 1977/2000, p. 34).

Put otherwise, driven by data and hosted by School, edtech can become the legitimate pedagogic power but also one that can "secure a monopoly of legitimate symbolic violence" (Bourdieu & Passeron, 1977/2000, p. 6). Moreover, with their advancement into education, edtech begin to emerge as the pedagogic power with technomonopolistic tendencies (Srnicek, 2017). That is, edtech can grow from a mediator of education to an influencer in the (re)production of education to a monopolist through the "expansion of [data] extraction, positioning as a gatekeeper, convergence of markets, and enclosure of ecosystems" (Srnicek, 2017, p. 98).

To this end, I adopt the concept of hypocrisy that emerges as edtech conflate with School's functions and, bringing Freire's (1970) critical pedagogy as my second angle of analysis, I argue that edtech present a hidden pedagogy of oppression, which "begins with the egoistic interests of the oppressors (an egoism cloaked in the false generosity of paternalism) and makes of the oppressed the objects of its humanitarianism" (p. 36). A sort of oppressive structure begets from such arrangements when privacy loss as the "new normal" of a datafied School conflates with edtech's commercial project for it (Figure 1). Losing one's privacy on privately owned data structures that are edtech can lead to children's dispossession of their own rights and freedoms in a supposedly sacred space for development of free thought that is School. The privacy loss in itself cannot automatically cause oppressiveness; losing privacy to data systems with their capacity to hypernudge and control the student can.

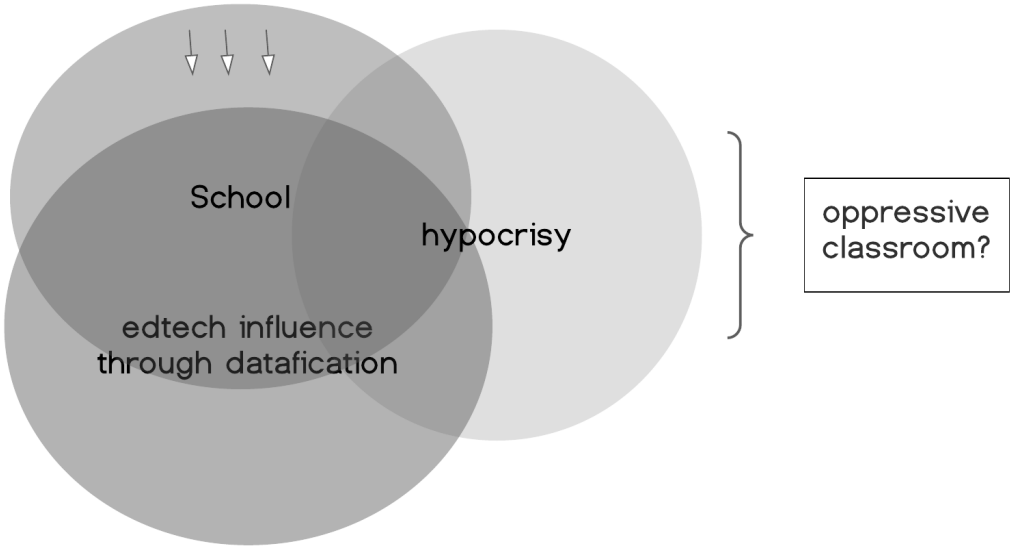

Figure 1. Edtech's pedagogic power hosted by School conflates with a sense of hypocrisy.

This rather pessimistic view of the climate in the datafied School leads to two objectives at which the article aims. First, it calls on School, in any shape and form that invests in and uses edtech products, educators, and policy makers, to reflect on the loss of privacy to which digitalized educational processes are leading and the subsequent complications for children's rights, freedoms, and futures. Unconsciousness toward edtech's growing legitimate power in School, while there is a lack of standard of edtech market regulation (Day, 2021), allows for their naturalization and challenges the efforts to understand and mitigate the subsequent risks to children's education and futures.

Second, for any data privacy literacy pedagogies to succeed, School should deploy a praxis of honesty through awareness, reflection, action, and resistance over data privacy practices and, equally, copartner with students in transforming the environment of hypocrisy and unconsciousness toward privacy loss to an honest one that is preserving it and maintaining independence.

The Importance of Privacy

Much ink is spilled about data privacy (Brunton & Nissenbaum, 2015; Nissenbaum, 2010) and the risks of harms from data privacy loss (Citron & Solove, 2021; Skinner-Thompson, 2021; Vèliz, 2021). The present intention is not to make an exhaustive account of why it is important and to whom. Within the context of School, the intention is to emphasize privacy as a deterministic *condition* for a growing child who is learning basic freedoms and rights within a *milieu*—that is School—where these freedoms and rights are practiced.

Privacy plays a critical role in the development of feelings, ideas, and identity (Warren & Brandeis, 1890). Privacy is also an incubator to development of thought, speech, and association. Neil Richards (2008) calls this intellectual privacy a "zone of protection that guards our ability to make up our minds freely" (p. 95). As School becomes wrapped by datafication systems, it begins to lose this zone of protection. The loss of privacy then leads to a wide range of risks (Citron & Solove, 2021; Reidenberg & Schaub, 2018) whose sheer volume begs the question: In what kind of new classroom climate do children learn?

As a condition, privacy also enhances individual autonomy. Informational and decisional privacy safeguard this autonomy by ensuring that one can control who has access to their personal information and to what extent (Westin, 1968), and one has the right against unwanted interference with their own decisions and actions (Lanzing, 2019). Without the condition of privacy, an individual cannot enjoy self-exploration and self-determination. Data collection from a child's assignment, a drawing, or behavioral conduct by an edtech application not only risks pinning the child into a data-derived category but also shifts the agentic power from the child to the data systems and their inferencing and surveillance capabilities. Thus, nudging and hypernudging (Yeung, 2015) become the modes of regulating behavior by design without a child's ability to control, resist, or refuse it. The data inferencing and surveillance capabilities present a form of oppression that is both at individual (how one practices self-expression and interprets what is learned) and structural levels (inferences derived from data influence curriculum decisions and what one should learn). Adopting these forms of education by School acknowledges them as legitimate power. This power drives a hidden pedagogy of oppression because it leaves few choices for the individual. One is to submit, perhaps remain fearful. Another option is to adopt and adapt to it. As Freire (1970) argues, the oppressed suffer duality:

> They discover that without freedom they cannot exist authentically. Yet, although they desire authentic existence, they fear it. . . . The conflict lies in the choice between being wholly themselves or being divided; between ejecting the oppressor within or not ejecting them; between human solidarity or alienation; between following prescriptions or having choices; between being spectators or actors; between acting or having the illusion of acting through the action of the oppressors; between speaking out or being silent, castrated in their power to create and re-create, in their power to transform the world. (p. 30)

The new oppressors watching over as individuals become ever more aware that the new reality will lead the oppressed to suffer this duality—either perform or hide, pretend or remain silent, and lose the ability and right to self-expression (Freire, 1970). In spaces other than School where data privacy loss is experienced, individuals have deployed various privacy defense mechanisms such as invisibility cloaks, finger prosthetics, and masks against pervasive technologies (Skinner-Thompson, 2021). But what are children supposed to do if they are to protect their own privacy in a classroom that allows privacy loss? Is the only "opt out" option to not attend School at all?

A third option, therefore, is to resist this new oppressive pedagogical power and to question it. Why, for example, is the pursuit of measurement through datafication seen as "highly desirable" and to whom (Beer, 2016, p. 3)? Why should profit-seeking businesses be trusted to define and solve School's problems—whatever these may be? What alternatives to datafication does School have for children?

While edtech are not in themselves automatically leading to privacy loss in School, their goal for massification across a market sector can lead to a form of *domestication* and their *legitimation*. They propose a new standard of "this is how things are done," which also domesticates one's critical faculties by a "situation in which [a student] is massified and has only the illusion of choice" (Freire, 1970, p. 31). The use of proctoring software for monitoring students' exams (Germain, 2020) during the COVID-19 pandemic lockdown, when most schools continued online and students remained home, is an example of creating the illusion of choice (taking a test while proctoring software monitors for cheating) and its massification that makes no room for student choice or voice (Hillman, Martins, & Ogu, 2021).

The illusion of choice prevails in college and career readiness platforms such as Naviance (PRNewswire, 2021). They have the capacity to restructure curriculum without children's participation and draw their future pathways (PRNewswire, 2021). A company like Naviance, owned by Hobson, is a data-collecting platform, which until it was sold to PowerSchool, a U.S. edtech, in February 2021, was a division of the *Daily Mail* and General Trust in the UK (Reuters, 2021a). Naviance collects a range of personal and sensitive information from personality surveys, students' interests, test results, parental employment history, income, and more. Additionally, it is part of a wider list of products including predictive analytics reporting, with ambitions to designing future career paths by "track[ing] students as they move through elementary school, college, and beyond" (Straumsheim, 2015, para. 1). Having previously acquired the National Transcript Center (NTC) software for electronic capture and exchange of student academic records between educational institutions, from Pearson Education, the international education and information company (PRNewswire, 2013), Naviance demonstrates not only how a business can tap into a tremendous amount of information about children but also the complex interchange among businesses within which student data are apprehended. See, for example, the recent merge of Anthology, which had already combined three higher-education administrative software businesses, with Blackboard, a learning management system (Lederman, 2021), demonstrating the power the combined company will accrue from its "ability to bring data from across the student lifecycle" (Lederman, 2021, para. 3). Importantly, it is on School's grounds where this apprehension begins. The choice to one's future becomes externalized and vested in the power of edtech (and their business owner of the day).

Is School a Private Space?

Proposing data privacy pedagogies demands some initial clarification about whether School is considered a public or a private space. While the duality itself is limiting, what students think and how schools present themselves to be would possibly generate as many nuanced responses as there are students and educational institutions.

Privacy principles and public discourse maintain that privacy rights are greatly diminished once one enters public spaces—when one leaves the privacy of their home and shares information with others (Cohen, 2019). School is certainly a space where one shares information with others within the bounds of its building. However, while a "stranger" cannot randomly walk into a School building without permission and justification (indeed, one must think about how children are taught about "stranger-danger"; Dixey, 1999, p. 40) in a datafied School, such sharing goes beyond its bounds over to hundreds of unknown individuals such as designers, programmers, agents, administrators, marketers, and business strategists, data analysts and brokers, and others who develop, manage, control, sell, repurpose, and own edtech (Barassi, 2020).

One possible answer to whether School is a private or a public domain is that it is private. In this case, edtech should be challenged when and how they are trespassing it. Together with students, School must negotiate clear boundaries and develop measures of keeping anyone from crossing them. For example, while American Student Assistance, a nonprofit organization, supports students in choosing education and career pathways, it also partners with Experian (2015), a global credit agency data broker, which has undergone numerous data breaches (Reuters, 2021b; Shange, 2020; Thielman, 2015). The data partnership among the two companies is not clear, and neither are the boundaries regarding children's data privacy.

If School, however, is considered a public space, then privacy becomes a contradictory term when one steps into its realm: One's privacy can no longer be guaranteed. Deciding what School *is*, it follows, will shape what children learn "private" and "public" mean. Once established as normative, these newly learned concepts become difficult to challenge (Skinner-Thompson, 2021).

Protecting one's privacy becomes even more complex when some doctrines link privacy with secrecy (Solove, 2006). Secrecy in public spaces carries a negative connotation—the sense that someone is hiding something inappropriate or wrong. Privacy is also understood as situational (Kaminski, 2019) or contextual (Nissenbaum, 2010). However, as much as contextual privacy provides a framework for thinking about the nuances associated with privacy, it also opens for business exploitations based on data extraction. For example, European and U.S. legal frameworks fail to prevent edtech's data exploitation, which risks children's privacy loss (Krutka, Smits, & Willhelm, 2021). Chromebooks used in public schools in the state of Virginia pass student information through Gaggle, an embedded scanning software, when it detects student content deemed inappropriate (Ray & Gentz, 2021). A school district may share academic data and attendance records with the local police, flagging possible future misconduct (McGrory & Bedi, 2020). Gaggle "analyzes the use of online tools within Google's G Suite, Microsoft Office 365, Google Hangouts, Microsoft Teams, and the Canvas learning management system for more than 4.5 million students across the United States" (Gaggle, 2021, para. 6). This demonstrates the cross-pollination of student

data among different edtech products that a school may be using. Gaggle (2021) declares: "Machine learning technology watches for specific words and phrases that might indicate potentially harmful behavior, flagging questionable content [which] is then evaluated by trained safety professionals to determine whether it is a threat—and how much of [it]" (para. 7). Such conditions risk becoming legitimized and domesticated as part of School's practices, while invisible hands[1] navigate these products.

Within the contextual privacy paradigm, students' academic records should maintain privacy within School's physical boundaries. Yet these are debased under the pretext of preventing future crime. The COVID-19 pandemic is now propelling the use of digital entry passes, designed by Microsoft (Blume, 2021), the corporation that employs more than 160,000 people (Liu, 2021). The entry pass collects data not only about children's physical state and whereabouts but also those of their friends and parents (Blume, 2021). Children's privacy in School is compromised as their data are exported to or combined with data from other corporate entities (e.g., Microsoft's [2021] privacy policy states: "We also obtain data about you from third parties"; para. 5), where other uses and laws may apply (Barassi, 2020). This reality depicts School as a public domain.

For healthy development, children require an environment that protects them from harm but also allows for exploration and discovery. However, like other seemingly safe spaces such as church, sports, and scouts' clubs, School has let horrific cases of child abuse (Renton, 2014). To estimate the risks of data privacy loss in a digital world more broadly, growing scholarship identifies tangible harms such as financial and physical, and intangible ones like vulnerability and emotional disturbance among others (Citron & Solove, 2021). However, practice shows that there is an overall struggle to recognize suffered harm when there is no tangible evidence. This delusion leaves countless privacy violations unaddressed (Citron & Solove, 2021). Software that scans students' Microsoft and Google accounts and homework, combined with machine learning, aims to detect "kids in crisis" (Turner, 2019, para 5), promising timely interventions for those in or causing trouble. The risks of harms from such surveillance practices themselves remain as afterthoughts (Kelly, 2019) and their effectiveness unclear (see, Gorard, Lu, Dong, & Siddiqui, 2021). If no tangible risk of harm from datafication and dataveillance is clearly defined in School, it follows that "*without lived privacy, one has no claim to legal privacy or privacy rights—and without legal privacy, one has no ability to protect or maintain lived privacy*" (Skinner-Thompson, 2021, p. 8; emphasis added).

[1] Indeed.com provides reviews from former Gaggle employees. While these merit further attention (who are the people working for edtech products?), the reviews suggest that to work as a safety representative at Gaggle is a low-wage job—a "side gig." One reviewer says:

> The basic lowest level representative (which you will start at) only has access to review documents. It's a[s] simple as reading a sentence and determining if it is urgent or harmful content. If you put in the hours and prove a near 100% accuracy rate, then you will be given additional responsibilities. (indeed.com, 2018).

Edtech's Project for School—A Hidden Pedagogy of Oppression?

The accelerating digitalization of educational processes impacts the social-structural organization of School profoundly. One way to look at edtech's project for School is that they claim pedagogic authority (Bourdieu & Passeron, 1997/2000). Edtech "manage to impose meanings and to impose them as legitimate" as they bring datafication as the remedy to School's ills (p. 4). Datafication legitimates and imposes meanings of what counts as learning. As such, edtech redefine learning through their reductionist and behaviorist prism (Manolev, Sullivan, & Slee, 2019). For example, the founder of Century Tech, a tutoring platform, promises learning improvement because her product allows it to *observe* "how students are behaving across the content" (British Broadcasting Corporation [BBC], 2021, 02:38–02:43). Others deploy psychological management techniques to model student behavior and adjust instruction accordingly (Manolev et al., 2019). Private global platforms like Google, Microsoft, and Amazon (Cavanagh, 2017) open prospects for transforming not only *how* curriculum is designed but also *who* designs it by collecting personal (meta)data about students across platforms and systems. By knowing more about students than they do or can reasonably be aware of and controlling how the data are processed, edtech create information asymmetries—the products of their pedagogic actions and work. Students simply cannot tell what is being done to them, by whom, and why: "The content inculcated is never seen in its full truth" (Bourdieu & Passeron, 1997/2000, p. 11). Additionally, there is no guarantee for how long any edtech "authority" might last. Therefore, edtech's project for School is highly experimental. For example, the Gates Foundation's InBloom project for collecting student data died within a year of its launch (Bulger, McCormick, & Pitcan, 2017). But edtech's experimental nature leads to many families' distress (Durkin, 2019; Parents Coalition for Student Privacy, n.d.) and teachers' protests (Courtney, 2018; see also Unite for Quality Education, n.d.; Badass Teachers Association, 2018).

While edtech provide many opportunities for School and learning, their project for either one is not necessarily driven by what is best pedagogically but by what is profitable (Teräs, Suoranta, Teräs, & Curcher, 2020). The growing financial value of behavioral data (Zuboff, 2019) presents opportunities for profit making. Data also have value to improve existing and developing products. The data sources are the users of digital systems; in education, these are the students. Students therefore can be seen more as data sources than "human beings" just as an oppressor would see the oppressed only as "things" (Freire, 1970, p. 39). To edtech, students become data sources for business growth. For example, Pearson Education earns millions from public education budgets for the provision, maintenance, and development of software (Commonwealth Data Point, 2016). Beyond this source of income, student data extraction helps businesses grow as Pearson plans a Netflix-style educational platform (Duke, 2021).

Freire argues that increasingly, the oppressive dominant force will use science and technology "as unquestionably powerful instruments for their purpose: The maintenance of the oppressive order through manipulation and representation" (Freire, 1970, p. 42). Mediating every School process and student interaction through edtech creates two powerful instruments that play at an oppressor's hand. First, technologies allow for every process, place, and person related to School to be mapped and known. To be known, one can be controlled. The true instrument of power is expressed when diminishing the choices for individuals to only two: Either be known or not—and perish in oblivion (Zuboff, 2019). To take a test, a student cannot opt out of the digital registration. The second instrument is making the first invisible. Digital

technologies interweave into everyday life in a way that one cannot see or distinguish them (Weiser, 1991), completing the hidden infrastructure. These two instruments strip not only privacy entirely; they establish the oppressive order and legitimize the new pedagogic power.

Measures of Safeguarding Privacy

(Lack of) Practical Measures to Safeguarding Privacy

While School is battling the strains of the pandemic, other sectors where digital intrusion diminishes personal privacy has called upon a whole generation of activists and inventors to invest their creativity in "the art and science of hiding" (Zuboff, 2019, p. 489). Zuboff (2019) emphasizes how "the intolerable conditions of glass life that compel these young artists to dedicate their genius to the prospects of human invisibility" (p. 489). The use of LED privacy visors against facial recognition (FR) cameras, quilted coats that block radio waves and tracking devices, and prosthetic face masks among other tactics exist for individuals opposing the "glass life" (Zuboff, 2019, p. 491). These are some of many examples detailed in recent literature (Skinner-Thompson, 2021; Vèliz, 2021). The sheer volume of techniques to protect personal privacy begs to make creative space in curriculum for practical approaches to data privacy literacy as School is steadily turning its walls to panes of glass through the deployment of surveillance software to catch cheating students (Germain, 2020), FR to collect attendance and monitor students' (Galligan, Rosenfeld, Kleinman, & Parthasarathy, 2020), and equally teachers' behavior (Strauss, 2013). Even without FR technology, surveillance of students now can take place through access to their laptops' cameras (Heddles, 2020).

If a practical consideration for teaching children data privacy literacy means to teach resistance against the "glass life," is there a flip side? Even if children resist surveillance, say, by wearing hoodies to cover from the prying eyes of cameras, resistance can backfire, pinning hoodie-wearing students for additional surveillance (McCahill & Finn, 2014). Student choice to maintain their own personal privacy remains illusionary. And so does the real choice for opt out. When students have no alternative about how to take an exam or make a career choice without edtech's influence, practical efforts to teaching data privacy literacy become inadequate.

Regulatory Measures to Data Privacy in School

Regulatory frameworks such as the General Data Protection Regulation (GDPR, 2016), the California Consumer Privacy Act (2018), the Colorado Consumer Data Protection Law (2018), and others are evidence of acknowledging children's privacy and measures of protecting it. However, as School emphasizes such legal defenses to be their benchmark of privacy provision for its schoolchildren in principle, in practice neither regulatory frameworks nor School succeeds in absolute privacy loss prevention as cyberattacks (Ram, 2021), data repurposing, and third-party access to School data continue (International Digital Accountability Council [IDAC], 2020).

If data privacy is needed to restore balance of power between those whose information is accessed and those who access and use it, there are at least three categories of danger that still need to be addressed.

Burton and Nissenbaum (2015) recall Donald Rumsfeld's statement that "there are known knowns, which we know we know; known unknowns, which we know we don't know; and unknown unknowns, which we don't know we don't know" (p. 48). An edtech application collecting (meta)data about a child may be known. How this data is repurposed is a known unknown. What follows are many unknown unknowns that regulatory frameworks do not—perhaps cannot—cover. A simple image captured by CCTV recording can lead to FR training software, which can further correlate with a credit card purchase or an entry to a library with a digital identity card, creating a level of insecurity—even unawareness (unknown)—that leads to other unknowns. This leaves loopholes in the privacy provision of School, which leads to what Burton and Nissenbaum (2015) conclude: "This isn't even the end of the unknowns, all potentially shaping consequential decisions produced in a dense cloud of our ignorance" (p. 49).

Pedagogical and Curriculum Measures for Data Privacy in School

It is understood that children's digital literacy plays an important role in how they understand, manage, and protect their privacy (Bulger & Davison, 2018). Defending one's privacy goes beyond merely providing, protecting, or withholding personal information. The commercial interest from data extraction (Zuboff, 2019) has led scholars to call for skills-based (Stoilova et al., 2021) as well as regulatory, tactical, and educational approaches to data literacies (Pangrazio & Sefton-Green, 2019). Educational responses have ascribed data literacy as an individual's ability to understand, identify, and engage in practical activities to demonstrate the level of skill acquisition. However, some critique that such efforts can fuse with the proliferation of other literacies ranging from media to coding, diluting the solutions to inadequate responses with limited success (Pangrazio & Sefton-Green, 2019). The proposal for pedagogic solution to data and privacy literacy is welcome among children (Stoilova et al., 2021). However, there is no knowledge about their view to privacy loss from datafication in School.

Developing a meaningful data privacy literacy curriculum should have a sense of clarity, which is that the dimension of privacy begins with School. First, it must be established what sort of private domain School *is*. An individual cannot simply walk into a school building without justification, identification, and so on. Similarly, a person cannot simply call themself a teacher, a doctor, or a school bus driver—they undergo training, licensing, and background checks before they teach, treat, and transport children. In contrast, edtech enter School and promise all kinds of improvements without licensing, background checks, or even evidence that their products work. Additionally, edtech data breaches (Page, 2021) increase the risk of exposing students' personal information and whereabouts, which can present physical risks.

Second, data privacy literacy pedagogy must strip down and display a growing "world of oppression" as edtech come to claim pedagogic power with their datafication practices, monopolistic tendencies, and destruction of personal privacy boundaries. Such pedagogy must give face and body to the invisible powers behind digital platforms and applications that provide pedagogy *for* the student. It must unveil what and who stand to benefit from children's interactions and preoccupations with edtech products. For while the child may learn with an intelligent system, the intelligent system learns from the child. On one hand, the risk is that the former will one day outperform the latter. The alternative to this risk is the mythmaking about such systems' "superhuman accuracy" (Campolo & Crawford, 2020, p. 1) that only reinforces their legitimate power in education. Children should know *that* side to edtech (Is their superhuman

accuracy a myth and a claim? Is their adoption the result of complacency, ignorance, or hypocrisy?). Third, data privacy literacy pedagogy should encourage children's own participation in the development of a pedagogy *with* them. Students no longer follow prescriptions, but have choices.

Problem-Posing Pedagogy for Data Privacy Literacy

The development of successful measures for data privacy literacy must begin by demolishing the hypocrisy bubble that engulfs School. This requires taking a step back. Growing scholarship in educational research more recently focuses on the narratives of compliance, surveillance, control, and acceptance of edtech (Decuypere, Grimaldi, & Landri, 2021). But there is something significantly lost when, in these debates, the focus shifts away from the fundamental functions of School and equally so—away from children's own voices and experiences. What is School supposed to do for a child? What are its functions? Then, within the debate of education technologies, what are edtech supposed to do for a child as they enter School, their market of interest (Fourcade & Healy, 2017)?

In the start of this article, School was expressed as any educational institution that provides certain functions. These functions can vary—from defining education to measuring it. Of course, its functions vary widely. Here, a difference must be made between School and education, which problematically conflate. Education is a lifelong process in which an individual learns to deal with the world, which can literally mean anything—from accepting to rejecting it, from manipulating to leading it, from understanding to explaining it. One can argue that educating one's self is one's own responsibility. The alternative is to get School's assistance. In this sense, School is accepted as something that provides an individual with assistance in getting educated. The quality in which School does it leads to judging whether it was done poorly or well. The former is likely to yield individuals who will gain no qualifications worth employability, learn no literacy, no value in inclusivity and justice, and may even drop out midway, unconvinced about School's purpose. A School doing its job well done should expect the opposite. School as an institution that assists one's education is like any other—church or prison, for instance. Just as church cannot guarantee a true believer, so cannot School guarantee well-educated individuals. As an institution, School invests resources and provides a system and a structure—it makes an investment, a sort of "banking" (Freire, 1970, p. 53). Children go to School, which in turn banks on their futures. One assumes that edtech businesses similarly bank on children's futures and promise a job well done when children use their products. These logics suggest that both School and edtech treat children as "receiving objects" (Freire, 1970, p. 58). A pedagogy that initiates such asymmetry only makes way for the world to allow for its fortification and ultimately the disenfranchising of students as ones who are not part of the world but ones who will eventually enter it. This notion explains the broader project of edtech with their interests to navigate students through a learning-to-earning framework of schooling (Deegan & Martin, 2018) where data are the primary sources that can make this framework possible.

The proposals for data privacy literacy in School therefore assume that children can—and should—become empowered against the opaque goals of the corporate world. But for such proposals to be truly successful, children have to be seen as cognizant, not as outsiders; as participants, not as receivers; as creators, not as depositories where material is transferred. An effective pedagogy for data privacy literacy therefore should assume an honest partnership and dialogue between teacher-student and School-student

where they "become jointly responsible for a process in which all grow" (Freire, 1970, p. 61) and are all in the world together where anyone has an equal chance to be negatively affected by data privacy loss and datafication. An effective pedagogy for data privacy literacy therefore demands problem-posing and problem-solving. To pose the problem means to unveil the reality (Freire, 1970)—the hypocrisy that arises as educational practices are gradually taking form proposed by edtech (Decuypere et al., 2021). Seeing the reality—and that both School and student are in it together—will pose the challenge to search for critical solutions. Within a pedagogy for data privacy literacy that is effective, individuals begin to

> . . . develop their power to perceive critically *the way they exist* in the world *with which* and *in which* they find themselves; they come to see the world not as a static reality, but as a reality in process, in transformation. . .the teacher-student and the students-teachers reflect simultaneously on themselves and the world without dichotomizing this reflection from action, and thus establish an authentic form of thought and action. (Freire, 1970, p. 64; emphasis in original)

No problem-posing pedagogy can work in tandem with the current climate of hypocrisy where edtech offer emergency solutions (Teräs et al., 2020) or "reimagined" pedagogies (Fullan et al., 2020, p. 3), because none of them allows those on the receiver's end (School and student) to begin to question them. Creating a free-of-oppression and privacy-preserving environment means not a mere reversal of position (e.g., expelling all edtech) or replacement, for the current regime only evokes previous oppressive ones (e.g., the ideologies gripping School when Nazism ascended; Mueller, 2020). Also, pedagogical and curriculum efforts for data privacy literacy should not look at data extraction and the risks of privacy loss outside School as though those risks are happening only independently, "out there" on the Internet or in the corporate world. They do not. They take place daily when a child enters the classroom, takes an exam, or converses with a friend on a shared Google document while at home. As such, data privacy literacy efforts must strip this *illusion* down and begin to unpack the data privacy *reality* of School. Thus, students, parents, and educators also have a *project* for School. Their input for its design should be included in the problem-posing pedagogy. Parents as well as teachers consistently demonstrate concerns for their children's privacy, objecting to edtech's aggressive commercial drive in education (see, for example, Parent Coalition for Student Privacy; Courtney, 2018; Mansell, 2019). These are important steps in the right direction—ones that form part of the problem-posing pedagogy—toward honesty and active participation, making School the sacred space for children to freely and independently build character and thought. A pedagogy for data privacy literacy must be a pedagogy that first dismantles the hypocrisy and demands that all oppressive practices are unveiled and assessed, not one that suggests freedom (through literacy) within a space that offers only the glass life and therefore an oppressive life.

Conclusion

If edtech claim to improve School processes, this makes them School experts. However, their claims are often more anecdotal, imbued with marketing discourse (Yu & Couldry, 2020) and powerful lobbying (Zuboff, 2019) for market share than having their teams occupying classrooms and examining school life and problems. Edtech enter schools with beta products without due trial and approvals by research boards or ethical committees or, indeed, without any substantial critical educational research on their impact

on the learning process, as well as how they are part of wider sociotechnical assemblages (Robertson, 2019). Software that reads students' personal messages enters the classroom without prior vetting or resistance (Beckett, 2019). If, indeed, improving learning were edtech's utmost priority (Fullan et al., 2020), what alternatives do they offer where children's data privacy is not compromised, data profiling and inferences do not have to be presented as a teachers' panacea, and automating future career pathways is not seen as a good thing? The choice seems to become more an illusion, as some have come to see School—as a "Microsoft" or a "Google" one.

Data-driven inferential teaching is a novel relationship imposed by the grammar of algorithms, which must be overcome. In Freire's words: "People educate each other through the mediation of the world" (Freire, 1970, p. 14) whereby the world, through its experiences, becomes the mediator, not the technology as might erroneously be assumed. A farmer can facilitate the learning process for a neighbor more impactfully and meaningfully than the algorithmic teacher brought in from outside. As such, technologies may condition the learning process, but the experiences and direct relationships with others mediate it. Through this new mediation do individuals begin to give meaning to the word and reclaim the right to say their own word.

The risk of subjugation by algorithms (Noble, 2019) brings up students to be objects that become the sum of their data who can be conformed to the logic of the algorithmic system. The subjugation is therefore elevated to a new *culture of silence* (Freire, 1970). This culture of silence becomes part and parcel of the hypocrisy—where School does not acknowledge, reflect, and act upon (or counter silence) about the data extractivism and edtech's commercialization emerging as dominant players in their very foundations. The realization of oppression from this new system of data-driven conditioning makes "real oppression more oppressive still" (Freire, 1970, p. 33). To avoid oppression from datafication, liberation, as Freire (1970) argues can partially be found through systematic education with the active participation of the oppressed. However, liberation must begin not only with students' active participation but with a pedagogy of honesty about the new power players claiming education as the "first frontier of a new societal territory" where "the youngest" are "its vanguard" (Zuboff, 2019, p. 436).

Reimagining education through technological innovation and its multimodal offerings grasps all sensors of a student. By extracting behavioral information, technologies also have the ability to redesign learning pathways, and from there—futures. An oppressed society comes to "feel an irresistible attraction towards the oppressors" (Freire, 1970, p. 45). A mentality risks becoming colonized. The digital transformation of educational processes looks to improve them, suggesting that something needs improving—an admission that there is inferiority, lack of capacity, and unproductiveness to which edtech offer solutions.

But technologies must be resisted through inquiry and their weaknesses assessed. School—student, educator, as well as policy maker—must see that any dominant force has its vulnerabilities. The vulnerability of the business of edtech must be acknowledged. Exporting its functions to the business sector makes School all the more dependent and vulnerable when such businesses fail. And businesses fail all the time (Johanes & Lagerstrom, 2017).

This article argued that to develop successful data privacy literacy pedagogies and curricula, first School—educators and policy makers—must see the social-structural changes edtech risk imposing as forms of oppression and as ways of claiming pedagogic power. Realizing this intellectually will not prevent or reverse the changes. Through the praxis of realization, reflection, and action, liberation, privacy preservation, and independent futures take place. Within such praxis, both School and students must engage in "cointentional education" (Freire, 1970, p. 51). That is, School as a social-structural establishment and its students must copartner in unveiling the hypocritical reality in which they coexist, a reality whose processes continue to be exported to edtech businesses, which ultimately risks relinquishing student autonomy. In such copartnership, *together with* School, can students see critically the risks of data privacy loss and "attain this knowledge of reality through common reflection and action [and] discover themselves as its permanent co-creators" (Freire, 1970, p. 51).

References

Andrejevic, M., & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology, 45*(2), 115–128. doi:10.1080/17439884.2020.1686014

Badass Teachers Association. (2018). Educator toolkit for teacher and student privacy: A practical guide for protecting personal data. *Badass Teachers Association*. Retrieved from https://drive.google.com/file/d/1__BcoGqrh24dWJiwdoyOv2TG3xX12_7x/view

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

Beckett, L. (2019, October 22). Under digital surveillance: How American schools spy on millions of kids. *The Guardian*. Retrieved from www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle

Beer, D. (2016). *Metric power*. York, UK: Palgrave Macmillan.

Blume, H. (2021, February 22). LAUSD to launch COVID-tracking app that generates a code for students to enter campus. Retrieved from www.latimes.com/california/story/2021-02-22/lausd-launches-daily-pass-app-track-covid-schools

Bourdieu, P., & Passeron, J. C. (2000). *Reproduction in education, society and culture* (2nd ed.). London, UK: SAGE Publications. (Original work published 1977)

Bozkurt, A., Jung, I., Xiao, J., Vladimirschi, V., Schuwer, R., Egorov, G., . . . Paskevicius, M. (2020). A global outlook to the interruption of education due to COVID-19 pandemic: Navigating in a time of uncertainty and crisis. *Asian Journal of Distance Education, 15*(1), 1–126. doi:10.5281/zenodo.3878572

British Broadcasting Corporation. (2021, September 4). *Click: Back to school* [Video]. BBC. Retrieved from https://www.bbc.co.uk/iplayer/episode/m000zglg/click-back-to-school

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: MIT Press.

Bulger, M., & Davison, P. (2018). The promises, challenges, and futures of media literacy. *Journal of Media Literacy Education, 10*(1), 1–21. doi:10.23860/JMLE-2018-10-1-1

Bulger, M., McCormick, P., & Pitcan, M. (2017). *The legacy of InBloom* (Working Paper 02.02.2017). *Data & Society*. Retrieved from https://datasociety.net/pubs/ecl/InBloom_feb_2017.pdf

California Consumer Privacy Act. (2018). *California Civil Code Division 3, Part 4, Title 1.81.5*. Retrieved from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Campolo, A., & Crawford, K. (2020). Enchanted determinism: Power without responsibility in artificial intelligence. *Engaging Science, Technology, and Society, 6*(2020), 1–19. doi:10.17351/ests2020.277

Cavanagh, S. (2017, May 8). Amazon, Apple, Google, and Microsoft battle for K–12 market, and loyalties of educators. *EdWeek Market Brief*. Retrieved from https://marketbrief.edweek.org/special-report/amazon-apple-google-and-microsoft-battle-for-k-12-market-and-loyalties-of-educators/

Cavoukian, A., & Castro, D. (2014). *Big data and innovation, setting the record straight: De-identification does work.* Ontario, Canada: Information and Privacy Commissioner*.* Retrieved from https://www2.itif.org/2014-big-data-deidentification.pdf

Citron, D. K., & Solove, D. J. (2021). Privacy harms (GWU Legal Studies Research Paper No. 2021–11). *Boston University Law Review, 102*(2). doi:10.2139/ssrn.3782222

Cohen, J. E. (2019). Turning privacy inside out. *Theoretical Inquiries in Law, 20*(1), 1–32. Retrieved from https://din-online.info/pdf/th20-1-3.pdf

Colorado Consumer Data Privacy Act. (2018). *H.R. 1128, 71st General Assembly*. Retrieved from https://leg.colorado.gov/bills/hb18-1128

Commonwealth Data Point. (2016). *Transparency at work in Virginia*. Retrieved from http://legacydatapoint.apa.virginia.gov/search_expenditure_detail.cfm?Vendor=Pearson&Agency=Department%20of%20Education%20-%20Central%20Office%20Operations&Object&Year=2017&fbclid=IwAR2eZSoZjPPWvbkW4vj8DINH636bP9nTeLQAdqrP0yhQ9hAwJYJoiDWEkPc

Couldry, N., & Mejas, U. A. (2019). *The costs of connection*. *How data is colonizing human life and appropriating it for capitalism*. Palo Alto, CA: Stanford University Press.

Courtney, K. (2018, May 31). *Teachers question taxpayer monies to support of for-profit education chain* [Video]. YouTube. Retrieved from www.youtube.com/watch?v=CA9U2exzyVc&t=4s

Day, E. (2021). Governance of data for children's learning in UK state schools. *Digital Futures Commission, 5Rights Foundation*. Retrieved from https://digitalfuturescommission.org.uk/wp-content/uploads/2021/06/Governance-of-data-for-children-learning-Final.pdf

Decuypere, M., Grimaldi, E., & Landri, P. (2021). Introduction: Critical studies of digital education platforms. *Critical Studies in Education, 62*(1), 1–16. doi:10.1080/17508487.2020.1866050

Deegan, J., & Martin, N. (2018). *Demand driven education: Merging work and learning to develop the human skills that matter*. London, UK: Pearson.

Dixey, R. (1999). What do mothers tell their children about stranger-danger? The place of health education and the creation of safer environments for children. *International Journal of Health Promotion and Education, 37*(2), 40–46. doi:10.1080/14635240.1999.10806092

Duke, S. (2021, October 14). App could transform Pearson into Netflix of the learning sphere. *The Times UK*. Retrieved from https://www.thetimes.co.uk/article/app-could-transform-pearson-into-netflix-of-the-learning-sphere-qb85zzllh

Durkin, E. (2019, May 31). New York school district's facial recognition system sparks privacy fears. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york-privacy-fears

Eisenstadt, M. (2021, April 13). *Amazon will give $1.75 million to new Syracuse STEAM high school*. Retrieved from https://www.syracuse.com/news/2021/04/amazon-will-give-175-million-to-new-syracuse-steam-high-school.html

Experian. (2015, October 27). *Experian partners with American Student Assistance to promote financial literacy to students*. Retrieved from https://www.experianplc.com/media/news/2015/american-students-assistance/

Fontichiaro, K., & Oehrli, J. A. (2016, May/June). *Why data literacy matters*. Retrieved from files.eric.ed.gov/fulltext/EJ1099487.pdf

Fourcade, M., & Healy, K. (2017). Seeing like a market. *Socio-Economic Review, 15*(1), 9–29. doi:10.1093/ser/mww033

Freire, P. (1970). *Pedagogy of the oppressed*. London, UK: Penguin Group.

Fullan, M., Quinn, J., Drummy, M., & Gardner, M. (2020). *Education reimagined: The future of learning. A collaborative position paper between new pedagogies for deep learning and Microsoft education*. Retrieved from https://edudownloads.azureedge.net/msdownloads/Microsoft-EducationReimagined-Paper.pdf

Gaggle. (2021, January 26). New data raises red flags about K-12 students' mental health during the pandemic. *Gaggle*. Retrieved from http://www.gaggle.net/press/new-data-raises-red-flags-students-mental-health

Galligan, C., Rosenfeld, H., Kleinman, M., & Parthasarathy, S. (2020). *Cameras in the classroom: Facial recognition technology in schools*. Retrieved from http://stpp.fordschool.umich.edu/sites/stpp.fordschool.umich.edu/files/file-assets/cameras_in_the_classroom_full_report.pdf

Germain, T. (2020, December 10). Poor security at online proctoring company may have put student data at risk. *Consumer Reports*. Retrieved from www.consumerreports.org/digital-security/poor-security-at-online-proctoring-company-proctortrack-may-have-put-student-data-at-risk/

General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union, 119*, 1–88. Retrieved from http://data.europa.eu/eli/reg/2016/679/oj

Heddles, C. (2020, September 25). Knox schools contract provides little protection over student data in some virtual classrooms. *WUOT The University of Tennessee Knoxville*. Retrieved from www.wuot.org/post/knox-schools-contract-provides-little-protection-over-student-data-some-virtual-classrooms

Hillman, V., Martins, J. P., & Ogu, E. C. (2021). Debates about EdTech in a time of pandemics should include youth's voices. *Postdigital Science and Education, 3,* 990–1007. doi:10.1007/s42438-021-00230-y

International Digital Accountability Council. (2020). *Privacy in the age of COVID: An IDAC investigation of COVID-19 apps*. Retrieved from https://digitalwatchdog.org/wp-content/uploads/2020/07/IDAC-COVID19-Mobile-Apps-Investigation-07132020.pdf

Johanes, P., & Lagerstrom, L. (2017, June 24). Adaptive learning: The premise, promise, and pitfalls. In *Proceedings of the 124th American Society of Engineering Education Annual Conference and Exposition (ASEE)*. Columbus, OH: ASEE. doi:10.18260/1-2--27538

Kaminski, M. E. (2019). The right to explanation, explained. *Berkley Technology Law Journal, 34*(1), 189–218. doi:10.15779/Z38TD9N83H

Kelly, H. (2019, October 29). School apps track students from classroom to bathroom, and parents are struggling to keep up. *The Washington Post*. Retrieved from www.washingtonpost.com/technology/2019/10/29/school-apps-track-students-classroom-bathroom-parents-are-struggling-keep-up/

Krutka, D. G., Smits, R. M., & Willhelm, T. A. (2021, March 18). Don't be evil: Should we use Google in schools? *TechTrends*. doi:10.1007/s11528-021-00599-4

Lanzing, M. (2019). "Strongly recommended" revisiting decisional privacy to judge hypernudging in self-tracking technologies. *Philosophy & Technology, 32,* 549–568. doi:10.1007/s13347-018-0316-4

Lederman, D. (2021, September 14). Blackboard, anthology to merge, creating EdTech behemoth. *Inside Higher Ed*. Retrieved from https://www.insidehighered.com/news/2021/09/14/blackboard-merge-anthology-creating-massive-ed-tech-company

Liu, S. (2021, August 3). Microsoft employee count 2005–2021. *Statista*. Retrieved from https://www.statista.com/statistics/273475/number-of-employees-at-the-microsoft-corporation-since-2005/

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society, 19*(5), 780–794. doi:10.1177/1461444816686328

Mandinach, E. B., & Schildkamp, K. (2021). The complexity of data-based decision making: An introduction to the special issue. *Studies in Educational Evaluation, 69*. doi:10.1016/j.stueduc.2020.100906

Manolev, J., Sullivan, A., & Slee, R. (2019). The datafication of discipline: ClassDojo, surveillance and a performative classroom culture. *Learning, Media and Technology, 44*(1), 36–51. doi:10.1080/17439884.2018.1558237

Mansell, W. (2019, January 25). 'It's a dictatorship': Angry parents fight back against school takeovers. *The Guardian*. Retrieved from https://www.theguardian.com/education/2019/jan/24/its-a-dictatorship-angry-parents-fight-back-against-school-takeovers

Masur, P. K. (2020). The politics of privacy: Communication and media perspectives to privacy research. *Media and Communication, 8*(2), 2183–2439. doi:10.17645/mac.v8i2.2855

Mayer-Schönberger, V., & Cukier. K. (2013). *Big data: A revolution that will transform how we live, work, and think*. London, UK: John Murray Publishers.

McCahill, M., & Finn, R. L. (2014). *Surveillance, capital and resistance: Theorizing the surveillance subject*. Abingdon, UK: Routledge.

McGrory, K., & Bedi, N. (2020, November 19). Pasco's sheriff uses grades and abuse histories to label schoolchildren potential criminals. *Tampa Bay Times*. Retrieved from https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/school-data/

Mueller, T. (2020). Heismeyer: Nazi education architect. *Journal of the History of Education Society, 50*(1), 50–66. doi:10.1080/0046760x.2020.1825832

Nissenbaum, H. (2010). *Privacy in context: Technology, policy and integrity of social life*. Palo Alto, CA: Stanford University Press.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism.* New York: NYU Press.

Page, C. (2021, August 16). Pearson to pay $1M fine for misleading investors about 2018 data breach. *Tech Crunch*. Retrieved from https://techcrunch.com/2021/08/16/pearson-to-pay-1m-fine-for-misleading-investors-about-2018-data-breach/

Pangrazio, L., & Sefton-Green, J. (2019). The social utility of 'data literacy.' *Learning, Media and Technology, 45*(2), 208–220. doi:10.1080/17439884.2020.1707223

Pangrazio, L., & Selwyn, N. (2020). Towards a school-based 'critical data education.' *Pedagogy, Culture & Society, 29*(3), 431–448. doi:10.1080/14681366.2020.1747527

Parents Coalition for Student Privacy. (n.d.). About us. Retrieved from https://studentprivacymatters.org

PRNewswire. (2013, July 11). *Hobson acquires National Transcript Center from Pearson*. Retrieved from www.prnewswire.com/news-releases/hobsons-acquires-national-transcript-center-from-pearson-215089041.html

PRNewswire. (2021, February 18). *Daily Mail owner sales its EdTech business Hobson for about $410 million*. Retrieved from www.reuters.com/article/us-dmgt-divestiture-hobsons-idUSKBN2AI2T5

Ram, P. (2021, March 3). Nova Education Trust: Online learning at Nottinghamshire schools hit by a sophisticated 'cyber attack.' *Nottinghamshire Live*. Retrieved from www.nottinghampost.com/news/local-news/online-learning-9-nottinghamshire-schools-5065769

Ray, K., & Gentz, S. (2021, August). *ESSA, Every Student Succeeds Act: Title IV funding guidelines* (White Paper). Retrieved from https://news.gaggle.net/title-iv-funding-guidelines-read?submissionGuid=a3721bb4-06df-4148-878d-7056998c3923

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education, 16*(3), 263–279. doi:10.1177/1477878518805308

Renton, A. (2014, May 4). Abuse in Britain's boarding schools: Why I decided to confront my demons. *The Guardian*. Retrieved from www.theguardian.com/society/2014/may/04/abuse-britain-private-schools-personal-memoir

Reuters. (2021a, February 18). Daily Mail owner sells its EdTech business Hobsons for about $410 million. *Reuters*. Retrieved from www.reuters.com/article/us-dmgt-divestiture-hobsons-idUSKBN2AI2T5

Reuters. (2021b, February 8). *Experian says investigating if involved in Brazil data breach*. Retrieved from https://www.reuters.com/article/us-experian-dataprotection-idUSKBN2A80MW

Richards, N. (2008). Intellectual privacy (Working Paper). *Texas Law Review, 87*, 387–445.

Robertson, S. L. (2019). Comparing platforms and the new value economy in the academy. In R. Gorur, S. Selalr, & G. Steiner Khamsi (Eds.)*, World yearbook of education 2019* (pp. 169–186). London, UK: Routledge.

See, B. H., Gorard, S., Lu, B., Dong, L., & Siddiqui, N. (2021). Is technology always helpful?: A critical review of the impact on learning outcomes of education technology in supporting formative assessment in schools. *Research Papers in Education*. doi:10.1080/02671522.2021.1907778

Shange, N. (2020, August 20). How Experian was duped into handing over data on 24 million South Africans. *The Sunday Times, South Africa*. Retrieved from https://www.timeslive.co.za/news/south-africa/2020-08-20-how-experian-was-duped-into-handing-over-data-on-24-million-south-africans/

Skinner-Thompson, S. (2021). *Privacy at the margins*. Cambridge, UK: Cambridge University Press.

Solove, J. D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.

Solove, J. D., & Schwartz, P. M. (2020). *Consumer privacy and data protection* (3rd ed.). New York, NY: Wolters Kluwer.

Srnicek, N. (2017). *Platform capitalism*. Cambridge, UK: Polity.

Stoilova, M., Livingstone, S., & Nandagiri, R. (2021). Data and privacy literacy: The role of the school in educating children in a datafied society. In D. Frau-Meigs, S. Kotilainen, M. Pathak-Shelat, M. Hoechsmann, & S. R. Poyntz (Eds.)*, The handbook of media education research* (pp. 413–425). Hoboken, NJ: John Wiley & Sons, Inc.

Straumsheim, C. (2015, February 23). Completing the 'student life cycle.' *Inside Higher Ed*. Retrieved from www.insidehighered.com/news/2015/02/23/student-success-company-hobsons-acquires-starfish-retention-solutions

Strauss, V. (2013, May 10). Bill Gates's $5 billion plan to videotape America's teachers. *The Washington Post*. Retrieved from www.washingtonpost.com/news/answer-sheet/wp/2013/05/10/bill-gatess-5-billion-plan-to-videotape-americas-teachers/

Teräs, M., Suoranta, J., Teräs, H., & Curcher, M. (2020). Post-Covid-19 education and education technology 'solutionism': A seller's market. *Postdigital Science and Education, 2*, 863–878. doi:10.1007/s42438-020-00164-x

Thielman, S. (2015, October 1). Experian hack exposes 15 million people's personal information. *The Guardian*. Retrieved from https://www.theguardian.com/business/2015/oct/01/experian-hack-t-mobile-credit-checks-personal-information

Turner, J. (2019, March 7). Tech software Gaggle finds possible pornographic item on Chesterfield Schools device. *NBC*. Retrieved from www.nbc12.com/2019/03/08/tech-software-gaggle-finds-possible-pornographic-item-chesterfield-schools-device/

UK Department for Education. (2020, April 24). *Schools to benefit from education partnership with tech giants*. Retrieved from https://www.gov.uk/government/news/schools-to-benefit-from-education-partnership-with-tech-giants

Unite for Quality Education. (n.d.). *A global response for commercialization of education*. Retrieved from https://www.unite4education.org/about/a-global-response-to-education-commercialisation/

United Nations Educational, Scientific and Cultural Organization. (2020). *Global education coalition: Members*. UNESCO. Retrieved from https://globaleducationcoalition.unesco.org/members

U.S. Department of Education. (2017, January). *Reimagining the role of technology in education: 2017 national education technology plan update* (Report). Retrieved from https://tech.ed.gov/files/2017/01/NETP17.pdf

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208. doi:10.24908/ss.v12i2.4776

Vèliz, C. (2021). *Privacy is power: Why and how you should take back control of your data*. London, UK: Bantam Press.

Warren, S. D., & Brandeis, L. D. (1890, December 15). The right to privacy. *Harvard Law Review, 4*(5), 193–220. Retrieved from https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Weiser, M. (1991). The computer for the 21st century. *Scientific American, 265*(3), 94–105. Retrieved from http://www.jstor.org/stable/24938718

Westin, A. F. (1968). *Privacy and freedom*. New York, NY: Athenum.

Yeung, K. (2015). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society, 20*(1), 118–136. doi:10.1080/1369118X.2016.1186713

Yu, J., & Couldry, N. (2020). Education as a domain of natural data extraction: Analyzing corporate discourse about educational tracking. *Information, Communication & Society*. doi:10.1080/1369118X.2020.1764604

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London, UK: Profile Books.