JIS Journal of Interdisciplinary Sciences
Volume 10, Issue 1; 59-80
May, 2026. © The Author(s)
ISSN: 2594-3405

The Surplus in Seeing: Networked Learning and Data Doubles in Parasitic Pedagogy

Jeremy Dennis
St. Louis Community College, USA
jdennis@stlcc.edu

Abstract: *Connectivism and networked learning continue to resonate as important approaches for advancing digital education. What is rarely considered is how parasitism and semiology underwrite these approaches and how their actualization privileges interpersonal or human collaborations while undervaluing nonhuman actants such as data doubles. As our information surrogates, data doubles manifest as byproducts of the surveillance and datafication of our personal information. This reconstitution is made possible by many of the same technology companies that permit networked learning and all digital interactions, thus allowing these establishments to feed on and profit from data extracted from us. This conceptual study reimagines parasitic pedagogy as a form of governance to explicate this process and challenge popular thinking about the relationship among networked learning, surveillance, and datatexts. As the master trope in parasitic pedagogy, the datatext formulates all digital objects, particularly data doubles. Although many educators neglect data doubles because of their opacity and unfamiliarity, technology companies increasingly treat them and their semiology as sources of surplus value, control, and extractive learning. To reveal how we have arrived at this paradoxical impasse, this study explores the philosophical and pedagogical character of parasitism and the Cold War political incentives that inspired the creation of the internet and many of the surveillance practices and data concerns that many educators have today. Parasitic pedagogy integrates these perspectives by illuminating their overlapping imperatives and practices, thus evidencing the ways in which technology companies and government agencies in the West and beyond often use the same fundamental technologies and networks as professional educators to propagate what Basil Bernstein called the totally pedagogised society.*

Keywords: Connectivism; data doubles; networked learning, pedagogic governance

Introduction

The influences and challenges associated with advanced technologies and learning management systems often inspire new articulations of pedagogy in the field of education (Bayne, 2024; Beetham & Sharpe, 2020; Demichelis, 2022; Dennis, 2020; Ross, 2023;

Siemens, 2017). Despite our competing appraisals of pedagogy at all levels of education, many practitioners seldom consider how its character might be expanded to explain phenomena outside of education. In fact, critics have claimed that, for some of us, "the term cannot travel beyond its category association with schools" (Sefton-Green, 2022, p. 902). However, influential theorists such as Bernstein (2000, 2001) and others challenge conceptualizations of pedagogy that limit its character to the theory and practice of teaching and learning in schools (Foucault, 2000; Giroux, 2004). For example, Bernstein (2001) introduced the concept *totally pedagogised society* to describe the ways pedagogy permeates all aspects of social life, including practices such as lifelong learning and evaluating the performativity of others beyond schooling. Thus, the totally pedagogised society signals the alignment of our worldviews and behaviors with the social relations and economic needs of the state as well as the corporate sectors it sustains (Dammann et al., 2022). Bernstein's concept explains how "governmental power is exercised through pedagogic means in the wide-ranging sense of cultural production–reproduction–interruption, and in the narrow sense of the everyday rituals of interactions between teachers and students" (Singh, 2017, p. 145). These relations are inherently pedagogical and techno-social, producing and reproducing symbolic control or governance through discursive formations or texts and the hierarchical relations that condition their development, reconfiguration, and circulation (Sefton-Green, 2022; Singh, 2017). Based on Bernstein's (2001) view of the totally pedagogised society, *pedagogic governance* can be characterized as a form of control that uses pedagogic means to regulate the transmission of knowledge, social interactions, and the semiology of identity and representation across populations (Foucault, 2000; Singh, 2017). Therefore, state–citizen and teacher–student pedagogical relations are entwined and treated as synonymous with others, including master–apprentice, master–slave, supervisor–supervisee, and trainer–trainee relations. To clarify this point, Singh (2017) reported, "Pedagogy and pedagogic relations—increasingly allied with technology—move outside the confines of state-centralised bureaucratic boundaries to constitute the primary or totalising binding agency of social cohesion" (p. 151).

In many ways, digital technology, internet platforms, and algorithmic systems enable new forms of governance (Tau, 2024; Tyler, 2004). In their assessment of Bernstein's work, Dammann et al. (2022) argued that advanced technology fundamentally transforms the way people are governed and how they govern themselves, particularly in the digital age. For them, pedagogic governance can be extended to include digital governance, data-driven governance, and algorithmic or cybernetic governance. However, Dammann et al. (2022) might agree that a Bernsteinian appreciation of pedagogic governance deserves more systematic inquiry and interpretation in relation to the surveillance, capture, and reconstitution of our personal information or data. In fact, scholars such as Singh (2017) also mentioned how little attention has been paid to explaining or expanding Bernstein's theory of the totally pedagogised society in education and beyond. "Given its potential importance," argued Tyler (2004), "it is unfortunate that Bernstein's reading of a society constituted by pedagogic processes lacks a well-articulated socio-semiotic framework on which such a radical vision could be based and its implications explored" (p. 15).

Therefore, this study attempts to address this gap in the academic literature by enriching our understanding of pedagogy as a form of governance that penetrates all aspects of our society. More specifically, I introduce *parasitic pedagogy* as an expression of pedagogic governance in which surveillance practices enabled by digital technologies and their communication networks extract our data and use those details to command knowledge and manifest our information surrogates or *data doubles*. As a result, our data doubles are often pedagogised, instrumentalized, and commoditized for the benefit of those who typically work outside the field of education (Williamson et al., 2020; Zuboff, 2019). Therefore, I reimagine the term parasitic pedagogy to describe the pedagogical and symbiotic relationship between data providers (hosts) and agents or organizations (parasites) that control data extraction systems that are increasingly used to govern us. In these systems, surveillance and digital technology are used to procure our personal information to reconstitute our physical bodies as information surrogates or data doubles for their surplus value or the vast amount of data that we supply as humans (Cole et al., 2021; Dennis, 2024; French & Smith, 2016; Serres, 1982). In Bernsteinian thought, this process is pedagogical in the sense that technology companies feed on our personal information to produce forms of knowledge and social relations that empower companies such as Google and Palantir and their algorithms and internet platforms. In turn, these companies use our personal information to circumscribe our agency as citizens, consumers, and learners (Giroux, 2015; Levine, 2018; Tyler, 2004). If educators want to fully understand parasitic pedagogy and its significance beyond our classrooms, then we need a better understanding of the historical contexts and incentives that have led to what seems to be an opaque or shadow system of interdisciplinary learning in which the proprietors of technology companies and their surveillance practices command digital infrastructures, internet platforms, and semblances of education that increasingly constrain our agency as humans and outpace our efforts as professional educators (Kim, 2022; Sefton-Green, 2022; Williamson et al., 2022; Zuboff, 2019).

With these concerns in mind, I will explore two interrelated questions in this study. The first question is, how can the Cold War political incentives that inspired the early development of the internet or Advanced Research Projects Agency Network (ARPANET) enrich our understanding of the current surveillance practices that manifest our data doubles and underwrite parasitic pedagogy? The second question is, what relevant insights about networked learning can be derived from an appraisal of parasitic pedagogy based on this historicization? To address these questions, I review the philosophical foundation of parasitic pedagogy and why scholars such as Patterson (2018) have referred to parasitism as a powerful paradigm for illuminating the semiotic properties that condition the relations of control between parasites and their hosts. More significantly, I reveal how digital technologies and their surveillance capacities increasingly trouble our systems of education, particularly because many of us advocate the use of learning management platforms, digital technology, and networked learning as popular tools for advancing and improving teaching and learning in the 21st century (Higdon & Bulter, 2025; Williamson et al., 2024; Zou et al., 2025). Depending on the context, the word *network* can be used to describe a system of webs, texts, or hypertexts—the markup language and links that make networked learning possible (Irvine, 2023; Landow, 2006). Moreover, the idea of *networked learning* is often associated

with connectivism and the work of thinkers such as Siemens (2017), Downes (2019) and others (Dennis, 2020; Ravenscroft, 2011). As a theory of learning, connectivism frames networked learning as practice. Generally, connectivism describes learning that occurs through a series of information nodes and links made across complex networks. It also refers to the interrelation of knowledge, digital resources, and interpersonal collaborations developed and supported by communication technologies and human learners in formal and informal environments (Downes, 2019; Siemens, 2017).

The Networked Learning Editorial Collective (NLEC) has updated and advanced an alternative conceptualization of networked learning. The NLEC (2021) is an international group of prolific scholars and researchers largely responsible for defining and advancing network learning as a field of study, discourse, and practice. According to the organization, networked learning involves "processes of collaborative, co-operative and collective inquiry, knowledge-creation and knowledgeable action, underpinned by trusting relationships, motivated by a sense of shared challenge and enabled by convivial technologies" (p. 319). Moreover, "Networked learning promotes connections: between people, between sites of learning and action, between ideas, resources and solutions, across time, space and media" (p. 319). With this description in mind, I reveal how the operation of *datafication* and *datatexts* or sign systems in parasitic pedagogy frustrates this characterization of networked learning and the popular support it tends to garner at all levels of education. To contextualize parasitic pedagogy as a counternarrative and expression of pedagogic governance, I examine how the history of the development of the internet or ARPANET and the Cold War political incentives that inspired its creation became the source and foundation of the digital technologies and communication networks that permit the appreciation of networked learning and digital education that NLEC and connectivism support. However, these early innovations also spawned the invasive surveillance practices that technology companies and government agencies have used to monitor and control our activities as consumers and citizens (Jacobsen, 2015; Levine, 2018; O'Mara, 2019). Also, these technologies and their infrastructure were originally imagined as teaching tools for research in the Department of Defense (War) then advanced as surveillance tools for managing the Cold War and insurgencies in the United States and abroad. More significantly, these innovations in digital technology and surveillance were later advanced and assetized by technology companies such as Google (Google Classroom), Palantir (Foundry), and others (Jacobsen, 2015; Karp & Zamiska, 2025; Tau, 2024; Ulbricht & Egbert, 2024; Williamson et al., 2022).

Based on this history, I explain why I consider datafication to be a parasitic and pedagogical process, particularly when technology companies and government agencies use digital technologies and questionable surveillance practices to manifest datatexts and data doubles for their own benefit while regulating or restricting privileges available to us. After evidencing and appraising these processes and practices as features of parasitic pedagogy, I discuss the key ideas in this study that suggest that the networked learning and digital education that many scholars and educators advocate are undermined by the parasitic practices of the technology companies they directly and indirectly support. More significantly, these practices reflect forms of governance that trouble networked learning as it

is promulgated by the NLEC, connectivists, and their supporters. Therefore, I recommend parasite pedagogy as an alternative discourse and starting point for framing and generating new understandings of networked learning outside the field of education. Additionally, I advocate parasitic pedagogy as a powerful interpretation of pedagogic governance and its operation beyond academic institutions.

Contextualizing Parasitism

Admittedly, the challenges that I conflate with parasitic pedagogy may not register for everyone because many educators do not necessarily associate companies with the cultivation and activation of pedagogy (Dennis, 2025c; Hinchliffe, 2001; Sefton-Green, 2022). However, this thinking is at odds with history and current events. For example, Hinchliffe (2001) claimed that since antiquity, pedagogy has represented a conceptualization of teaching and learning organized to service government, political power, and the economy. Surveillance or monitoring has often been at the core of this formation. As a marker of pedagogic relations, surveillance is inherent in the practice of teaching, increasing its efficiency and disciplinary power (Foucault, 1995). In fact, it is through surveillance that discipline becomes an automatic and anonymous form of power, integrated to function like a network of relations that doubles as a system of governance and control (Dennis, 2025b; Foucault, 2000). Artificial intelligence and emergent technologies have granted surveillance a new momentum and ubiquity. Giroux (2015) claimed that surveillance by corporate and government entities has warranted closer analysis because it inhabits our everyday activities to the point where it is often taken for granted. In fact, the increasing ubiquity of surveillance permitted by digital technology also expresses pedagogic governance (Dammann et al., 2022; Foucault, 2000). In other words, the reconstitution of our physical bodies as digital data, knowledge, and commodities is made possible by surveillance systems embedded in and facilitated by algorithms, smart devices, and internet platforms (Bayne & Jandrić, 2017). Government agencies and technology companies such as Google increasingly use these systems to collect, aggregate, and instrumentalize our personal information to monitor and moderate our behavior (Giroux, 2015; Lamdan, 2023; O'Mara, 2019; Tau, 2024). Therefore, these organizations and the technological programs and infrastructures that they control feed on the data derived from our personal information and social interactions as we live and learn in formal and informal settings (Knox, 2021; Tau, 2024). The incessant mining, recording, and recombination of data extracted from us for the benefit of others move us beyond the traditional conceptualization of pedagogy as the art and science of teaching and learning in schools to an appreciation of its character as a form of governance that creates a totally pedagogised society (Dammann et al., 2022; Gourlay, 2021; Knox, 2021; Tyler, 2004; Williamson et al., 2022).

For example, French and Smith (2016) claimed, "An ontology of the body as a reliable organism for identification and measurement has helped turn bodies into focal points for practices of monitoring and control" (p. 8). Technology companies as well as government agencies exploit the patterns found in data provided by or extracted from us to control our

agency as citizens, consumers, and learners. Therefore, our bodies are swapped out by surveillance systems in favor of more malleable and mobile representations or doppelgängers (French & Smith, 2016; Pierlejewski, 2020). In this dynamic, our bodies are rearticulated and reorganized to function as information surrogates that manifest as byproducts of the digital translation and transformation of our personal information into data that can be curated, stored, and endlessly recombined for the benefit of others (Beck, 2015; French & Smith, 2016; Knox, 2021; Pierlejewski, 2020). More significantly, this illustration explains how our human identity is multiplied by surveillance practices facilitated by the computers and smart devices that we engage in our everyday lives, thus feeding, cultivating, and advancing the vast technological and surveillance systems that give life to the information surrogate or data double used to circumscribe the physical body. Pedagogically, this relationship is not about what can be taught and learned per se, but how the data about us can be deployed to produce the knowledge, pattern analytics, and surrogates that others can use to manipulate and govern our life chances and sovereignty (Bayne & Jandrić, 2017; Bernstein, 2001; French & Smith, 2016).

It is in this context that the various technologies and surveillance protocols used to transform our bodies and lives into data for the benefit of others begin to reflect *parasitism.* The term parasite sits at the core of its conceptualization. According to Botz-Bornstein and Stamatellos (2022), a parasite is an organism that requires another organism or host for life, growth, and survival. As a philosophical phenomenon, parasitism probes the ethical, biological, and semiological attributes of a parasite as metaphorical, technological, or pedagogical considerations (Cole et al., 2021; Kim, 2022; Serres, 1982). In ancient Greek philosophy, we find references to the effects of parasites and parasitic thinking in the works of philosophers such as Aristotle. In fact, Aristotle ascribed political connotations to the word *parasitos* to refer to *abiogenesis* or the sudden generation of life out of non-living matter (Botz-Bornstein & Stamatellos, 2022). However, philosophical and para-philosophical references to parasitism are often associated with the work of contemporary philosophers such as Serres (1982). For Serres, the representation of the host on which the parasite depends is doubled. In one vignette, he characterized the relationship as follows: “The host, the guest, breathes twice, speaks twice, speaks with forked tongue, as it were.” Parasites and hosts are always in “the process of passing by, being sent away, touring around, walking alone. They exchange places in a space soon to be defined” (Serres, 1982, p. 16). Thus, metaphorically, parasites can be agents or organizations that initiate and organize semiology and communication between parts, a process that conditions how we understand the depiction of the whole by making it possible in the first place (Dennis, 2024; Kim, 2022). Based on this assessment, parasitism is ultimately a theory of relations and networks represented by a chain of signs or units of communication and the representations they produce—which are fundamental to our understanding of human and nonhuman relations and networked learning in the digital age (Bayne, 2024; Beck, 2015; Botz-Bornstein & Stamatellos, 2022; Ravenscroft, 2011; Serres, 1982). This view is supported by the work of Patterson (2018), who argued that parasitism ranges from minor dependences to major forms of exploitation such as enslavement. He introduced the term *human parasitism* to help illuminate this insight and describe the inherent exploitation and inequality often embedded in asymmetrical human relations and exchanges.

Furthermore, these relations are usually conditioned by tension, conflict, and the simultaneity of differences. In this instance, parasitic relations enable levels of engagement and synchrony akin to the networks and constituting power that we associate with hypertexts as the markup language, links, and infrastructure through which digital technology, texts, and data signify, constitute, and recombine (Dennis, 2020; Landow, 2006; Siemens, 2017).

Hypertextuality is also used to describe how texts and links drive the digitalization and datafication processes in which all social phenomena and materialities are translated and transformed into digits and data that algorithms, computers, and computerized devices can recognize, modulate, and circulate at will (Gunkel, 2018; Landow, 2006). Vast systems or networks of hypertextuality connect all digital expressions and link a range of observations, contradictions, and relations of power that condition data and their different representations. In this instance, data—like texts—represent sign systems that signify concrete materialities as they are represented in analog or digital forms as well as verbal and nonverbal expressions of thought, intersubjectivity, and communication. Like texts, data also constitute systems of exchange that permit the translation and circulation of knowledge and information about human and nonhuman relations (Benoit, 2020; Dennis, 2025a; Gourlay, 2021; Ravenscroft, 2011). Thus, I introduce the term datatext to describe the systems of communication, connection, and collaboration that express parasitism, new forms of (dis)embodiment, and (hyper)textuality as they exist in the digital world and virtual environments (Benoit, 2020). In his study, Dennis (2024) indicated that, like any form of text, hypertexts are also constituted by signs or units of description that always refer to something other than themselves. This heterogeneity is generated by their parasitism and incessant reformulations that support the social relations, exchanges, and networks that give them life. Once we are ensconced within a network of hypertexts for teaching, learning, or surveillance, our personal information and other materialities no longer exist or advance on their own. To clarify this point, Landow (2006) noted that any text or document, however defined, placed in any networked system supported by hypertexts or electronically linked materials will exist in collaboration with all other texts in that system. Therefore, all texts digitally networked to other texts always collaborate and communicate in ways that reflect parasitism (Patterson, 2018; Zuboff, 2019).

Parasitism and Surveillance Education

In parasitism, a networked system driven by digital technology, though beneficial, is simultaneously one of exploitation, contradiction, and historicization. In turn, this system conditions the historicity of knowledge and contextualizes controversies and problems related to the internet and its infrastructure (Dammann et al., 2022; Foucault, 1995; Landow 2006). However, the history, incentives, and troubling collaborations that led to the design and instrumentalization of the internet and the digital technology, complex networks, and surveillance systems it supports are often missing in the academic literature on surveillance in education (An & Oliver, 2021; Levine, 2018). In fact, today's surveillance society and accompanying practices emerged from a surveillance-industrial complex, according to scholars such as Ball and Snider (2013). The Cold War and the military and corporate

prerogatives it often prioritized cultivated the system that would eventually underwrite the parasitism, data assemblages, and human (dis)embodiment discussed earlier. For Ball and Snider and others, surveillance enables the increasingly ubiquitous means and contexts in which our personal information is collected, judged, and managed by different organizations and institutions, including schools (Dennis, 2026; Lyon, 1994, 2022). These establishments often recognize us by our data or the coded sequences of our personal information translated into numbers that computerized machines and devices can efficiently coordinate and manage. Lyon (1994) claimed that the databases of large companies and government agencies permit the storage, processing, and retrieval of precise details about our personal lives and habits. More specifically, he pointed out how government agencies in the United States military and security agencies developed large computers and information networks that led to the ubiquitous forms of digital surveillance and social control that remain operable today. For many government officials who oversaw the development of early computing systems and large databases, surveillance was a means for exercising control rather than advancing democracy (An & Oliver, 2021; Levine, 2018; Lyon, 1994, 2022). Consequently, the rapid rise of these systems and their communication networks—which eventually produced the internet—increased fears that these innovations would become repressive surveillance tools. This sentiment tended to contradict advocates who regarded these technologies as benign or convivial instruments for transcending class biases, social inequality, and racial discrimination (Giroux, 2015). However, Levine claimed, "By pretending that the Internet transcends politics and culture, we leave the most malevolent and powerful forces in charge of its built-in potential for surveillance and control" (p. 274). The same assessment could be made about studies of surveillance in education that fail to feature or consider historical contexts that help to explain the problems associated with the very surveillance and information systems they recommend for comprehensive critique and reform.

For example, several scholars have noted that online learning and learning management systems that facilitate networked learning and digital education embed surveillance systems that track data related to the activities and habits of students and teachers as part of the pedagogical and governing function of technology in education (Beetham et al., 2022; Dennis, 2025b; Higdon & Butler, 2025; Gilliard & Selwyn, 2023; Land & Bayne, 2005; Williamson et al., 2024; Zou et al., 2025). The efficiencies and conveniences associated with these systems and practices are often used to quiet critics who warn about the data extraction and parasitism these technological systems enable, the privacy and data security measures they warrant, and the forms of inequality they help reproduce due to some students' lack of access to the technological infrastructures needed to support networked learning and digital education (Beck, 2015; Dennis, 2024; Gilliard & Selwyn, 2023; Nemorin, 2017; Zou et al., 2025). As indicated earlier, the normalizing impact of surveillance in education is not a new phenomenon. However, the growing use of internet platforms and the automation of modern surveillance in schools increasingly rely on the datafication of information about students and teachers as a form of governance, market capture, and profit maximization (Higdon & Butler, 2025; Knox, 2021; Williamson et al., 2022). These surveillance practices are extractive and exploitative in nature and intent, shifting the surplus value found in educational data into the

private sector (Beetham et al., 2022). However, this managerial ethos—which is often associated with the use of learning management systems and internet platforms in education—tends to normalize the learner as a unified subject instead of one who is heterogeneous and semiotic. In this context, the term *semiotics* characterizes the construction of the self by a system of fluctuating signs and their multiple meanings or significations in different contexts (Peirce, 1955; Semetsky, 2017). The semiotic learner is antithetical to the certainty and objectivity that administrators often hope to achieve with surveillance practices that generate analytics for data-driven education (Land & Bayne, 2005; Semetsky, 2017; Williamson et al., 2020).

In their study of surveillance in education, Monahan and Torres (2010) argued, "At its root, therefore, surveillance is not simply about monitoring or tracking individuals and their data—it is about the structuring of power relations through human, technical, or hybrid control mechanisms" (p. 2). In their assessment of these relations and others, Higdon and Butler (2025) suggested that many surveillance practices in education are exploitative and antithetical to a pedagogy of emancipation or participatory democracy as it is advanced by many progressive scholars and educators (Giroux, 2004; NLEC, 2021; Schick & Timperley, 2022; Williamson et al., 2020). In fact, developments in these areas—particularly for those who study networked learning—are often overshadowed by critiques of technological evangelism and the capitalistic and parasitic practices of agents in the educational technology industry (NLEC, 2021; Williamson et al., 2020). This might explain why scholars such as Higdon and Butler (2025) have supported and advanced the use of critical media literacy as a framework to examine the impact of surveillance in education and the predatory nature of those technology companies that increasingly cater to academic institutions. However, for Land and Bayne (2005), a completely different approach to pedagogy may be necessary. They argued that technological considerations of new modes of identity formation and power relations may be a significant route for developing effective pedagogies for teaching and learning in the digital age. To further complicate matters, Beetham et al. (2022) insisted that a broad range of research is needed, including "more theoretical and empirical attention at a systems level" (p. 30).

Ironically, in their competing assessments and recommendations, these scholars seldom advocated investigations of the historical contexts and incentives that have produced the technologies and surveillance systems that they all agreed are problematic (An & Oliver, 2021; Dennis, 2025c; Lewin & Lundie, 2016). More specifically, when scholars such as Giroux (2015) and Higdon and Butler (2025) did mention the role that the U. S. military, security, and corporate agents have played in developing and advancing the vast technological and surveillance systems that we experience today, they present tertiary rather than foundational considerations. Without an adequate historical context, we are unable to recognize or address the forms of parasitic pedagogy that exist within and beyond our classrooms (Bayne & Jandrić, 2017; French & Smith, 2016; Tau, 2024). This brings us to the two questions that will be explored below. This first question is, how can the Cold War political incentives that inspired the early development of the internet enrich our

understanding of the current surveillance practices that manifest our data doubles and underwrite parasitic pedagogy? The second question is, what relevant insights about networked learning can be derived from an appraisal of parasitic pedagogy as practice based on this historicization?

Historicizing Modern Surveillance Practices

How we arrived at laptop computers and smart devices networked by the internet is a story of Cold War counterinsurgency initiatives and technological innovation (Irvine, 2023; Jacobsen, 2015). It is also a story that reveals how surveillance emerged as the ubiquitous force that it is today. Whether we use the internet and its vast networks for directions, dating, or email, it has always had a complex nature as a tool for intelligence gathering and war (Levine, 2018). The internet as we know it today began as ARPANET, a program developed by the U. S. Department of Defense's Advanced Research Projects Agency (ARPA), which is currently known as the Defense Advanced Research Projects Agency (DARPA). Scholars have noted that historians tend to differ when it comes to the fundamental causes that led to the creation of the internet (Levine, 2018; O'Mara, 2019). However, what remains clear for some is that early computers and their complex communication networks were viewed as teaching tools for personnel in the U. S. Department of Defense. According to an internal report for ARPA, "Computer assisted teaching systems and computer assisted gaming and simulation studies are examples of work chosen [for] human performance research believed to be defense relevant" (as cited in Jacobsen, 2015, p. 152). The need to fight Communism and insurgents abroad presented an opportunity for ARPA to demonstrate how technological innovations and surveillance could be operationalized and pedagogised to serve the prerogatives of the U. S. military and security agencies, particularly during the early stages of the Cold War.

At the beginning of the Cold War, the United States was a preeminent global power, overseeing an increasingly volatile world. At the time, presidents and key defense officials wanted a more effective means for countering Communism around the globe. ARPA proved to be an ideal resource for achieving this goal. Accordingly, computer-aided information and surveillance technology could be used to surveil, study, and understand the culture of insurgents around the world to discover what motivated their resistance and what could be done to prevent it from metastasizing (Jacobsen, 2015; Levine, 2018). The idea was to use advanced computer-aided information and surveillance technology to help the United States respond to insurgencies. It was also a spy tool for learning as much about the enemy as possible, including *their* behaviors, hopes, fears, social networks, and proximities to power (Jacobsen, 2015; Levine, 2018). Later, the same computer-aided information and surveillance technology was used to surveil and subdue those considered insurgents inside the United States, particularly activists associated with the Civil Rights Movement and activists against the Vietnam War. Ironically, around the same time that professors, scientists, and engineers were marshalled to build a unified military computer network, Levine (2018) claimed that the United States was being disrupted by protests, violence, militant Black activism, and left-wing student movements. Fearful, the American establishment felt a response was warranted

that was as effective as the counterinsurgency plans the U. S. military and security agents used abroad. Therefore, ARPA was adapted to address so-called *domestic enemies*, which increasingly came to include any individual or group agitating for socioeconomic equality, social justice, and democratic political engagement (Jacobsen, 2015; Levine, 2018). Levine (2018) reported, "There was no doubt: the ARPANET was being used to monitor domestic political activity" (p. 90). In fact, it was not uncommon to find officials who developed and advanced ARPA in Vietnam returning to the United States to apply similar counterinsurgency strategies and tactics to prevent or manage domestic problems spawned by years of racial injustice, economic inequality, and depoliticization. The approaches used by ARPA and its domestic agents often involved the surveillance, collection, and circulation of personal information about innocent and law-abiding citizens. This might explain why authors such as Levine (2018) have argued that the internet was designed to be an instrument for surveillance and governance from the start. It emerged out of "an attempt to build computer systems that could collect and share intelligence, watch the world in real time, and study and analyze people and political movements with the ultimate goal of predicting and preventing social upheaval" (Levine, 2018, p. 7).

As the predecessor to the internet, ARPANET was also interdisciplinary in the sense that it integrated—and sometimes weaponized—sciences such as sociology, mathematics, engineering, psychology, and semiotics, thus putting the academic disciplines and knowledge in the service of American foreign and domestic policy (Irvine, 2023; Levine, 2018; Tau, 2024). In one study, Irvine (2023) claimed that computing and semiotics have been interconnected since the late 17th century. Originally, the term *computer* often meant a person who did calculations using a system of signs animated by symbols and numbers. As a result, humans and the semiology they represented became blueprints or models for the central processing units used in computers (Irvine, 2023). Therefore, semiotics was often considered an essential prerequisite for modern computing and the programming languages that our computer systems use today—even though their semiotic character and principles are often opaque and understudied. Nonetheless, Irvine (2023) and Landow (2006) indicated that hypertextuality and its semiology operationalize digital texts and connect internet users and servers. This process allows computer systems to function using a vast communication and meaning-making network in which signs are produced, constituted, and mobilized to form the semiology supporting the networking protocols that permit the translation and distribution of data as well as networked learning and digital education (Dennis, 2025a; Gunkel, 2018; Irvine, 2023; Land & Bayne, 2005). This dynamic might explain why Semetsky (2017) has suggested that semiotics traverses the walls of formal educational settings, inaugurating posthuman dimensions of learning in which a relational self can be formulated out of signs or what we typically call *data*.

However, what is understood by the term *data* has changed throughout history. Kitchin (2021) pointed out that data derived from the Latin word *dare*, which means "to give." As late as the 17th century, data were used in the English language to denote anything widely known or generally accepted. In the 20th century, data became increasingly associated with computing and technology, describing information that can be abstracted, measured, and

stored for coding, pattern analytics, and machine learning (Benoit, 2020; Dennis, 2026; Kitchin, 2021; Lamdan, 2023). In the 21st century or digital age, data points are increasingly characterized and treated as signs and synonyms for material and non-rival resources such as information, knowledge, texts, and writing (Dennis, 2025b; Lamdan, 2023; Peters, 2023). On the other hand, many view data as comprising assets and forms of power and property that rival land, money, and machines. For example, Sadowski (2019) argued that collections of data are the recorded abstracts of the world and material resources that can be used to manage, reorganize, and control things, including information, money, and people. The idea is that amassing data about an object grants one the ability to exercise power over it, thus permitting the extraction of more data. Therefore, the flow of data often corresponds to the flow of power and capital, making the circulation, storage, and analysis of data central features of modern capitalism and governance (Peters, 2023).

In these contexts, it is the semiotic nature of data that facilitates the production, translation, and distribution of the computer-aided information and surveillance technology originally developed by ARPA. More significantly, semiotics offers us a way to contemplate the ways in which data—as a system of signs—can simultaneously represent knowledge, information, and texts processed by humans or nonhumans such as computers (Dennis, 2026; Gunkel, 2018; Irvine, 2023). It was in the development of computer-aided information and surveillance technology by ARPA that we increasingly see nonhuman tools in the form of computerized machines being used to collect data, create databases, produce predictive models, and share that information across space and time (Levine, 2018; Tau, 2024). Lyon (1994) described a database as a system for processing and warehousing data for selective retrieval and distribution. As sign systems, data and databases are discursive, textual, and relational, allowing us to link and integrate them in different ways (Irvine, 2023; Land & Bayne, 2005). Thus, networks permitted by data and databases may be the most significant innovation the U. S. military and security agencies modeled for the corporate sector. For some, the late 1960s marked the start of a computerized gold rush in the United States. Government agencies, intelligence services, and large corporations began to computerize, digitize, and advance their operations in innovative ways (Levine, 2018; O'Mara, 2019). As a result, government and corporate databases proliferated across the United States and beyond. Digital databases and networked computer systems increased the efficiency of American corporations and reduced their labor costs. Also, several technology companies were redeveloped into powerful organizations that often partnered with the U. S. military and security agencies while tracking and profiling us using methods not too distant from those used by ARPA agents (Levine, 2018; Tau, 2024).

In fact, Levine (2018) reported, "Some parts of these companies are so thoroughly intertwined with America's security services that it is hard to tell where they end and the U. S. government begins" (p. 5). The increasing privatization of the internet, despite its origination as a military and intelligence tool focused on counterinsurgency at home and abroad, has grown into a complex ecosystem that spans every kind of computer network and data system imaginable. Therefore, as more of our lives take place online, the semiology or trails of digital data left behind are increasingly recorded, curated, and leveraged for their

surplus value by technology companies as well as governments (Kitchin, 2021; Levine, 2018; Tau, 2024). What may be most significant in this transformation is that these technological innovations and their digital surveillance capacities have allowed technology companies such as Google to move into the education sector using their technological resources, software tools, and infrastructural might, thus encouraging the digitalization of academic operations and the prospects for a totally pedagogised society (Dennis, 2025b; Knox, 2021; Williamson et al., 2020). In fact, the number of companies that specialize in educational technologies has increased, thus authorizing their digital devices, platforms, and programs to legally access and capture academic data on minors, which they might otherwise be prohibited from accessing. Higdon and Butler (2025) added, "Recognizing the lucrative opportunity for mass data collection posed by compulsory schooling, big-tech companies seek to enter the classroom and find success by offering economic incentives to educators and 'free' or low-cost devices for students such as laptops, tablets, and Chromebooks" (p. 9). Although some may see this as a form of corporate benevolence, others might view it as further evidence of parasitism and the commercialization of teaching and learning (Dennis, 2024; Higdon & Butler, 2025; Williamson et al., 2022)

However, there are other concerns. For example, some critics have reasoned that the long-term goal of many technology companies is to use algorithms and predictive analytics to triangulate and instrumentalize data about teachers and students in a greater effort to predict and control every aspect of human behavior (Higdon & Butler, 2025; Tau, 2024; Zuboff, 2019). Scholars in education, including the philosophy of education, have called attention to this growing problem and its consequences. However, many of them tend to focus on philosophies of digital pedagogy and seldom consider philosophies related to parasitic pedagogy (An & Oliver, 2021; Beetham & Sharpe, 2020; Lewin & Lundie, 2016; Sefton-Green, 2022). The reason for this inattention may be that not many scholarly studies consider or explore parasitic pedagogy and its semiology inside the field of education or beyond (Beck, 2015; Cole et al., 2021; Dennis, 2024; Knox, 2021; Semetsky, 2017). Schick and Timperley (2022) and others have argued that scholars often underappreciate the fact that pedagogy routinely happens in locations outside schools and classrooms in both intentional and unintentional ways. Therefore, they might agree that pedagogies outside the field of education deserve more attention, and these pedagogies should be understood and framed to clarify how we learn, relate, and act (Schick & Timperley, 2022). The challenges in achieving this initiative revolve around our different starting points. On the one hand, educators focus primarily on teaching students or humans (Bayne & Jandrić, 2017). On the other hand, technology companies appear more interested in the nonhumans that function as information surrogates or data doubles for students, teachers, and everyone else (Beck, 2015; Dennis, 2025b). As a result, a new anthropological and pedagogical form has been inaugurated by the innovations initially developed by the U. S. military and security agencies and later advanced by technology companies such as Palantir—a company that specializes in surveillance and the integration, analysis, and operationalization of data worldwide (Dennis, 2025a; Gourlay, 2021; Karp & Zamiska, 2025; Ulbricht & Egbert, 2024).

Using digital surveillance and internet platforms, these technology companies as well as government programs can use our data doubles to monitor and govern our behaviors and actions. The digitalization of data often refers to a process in which digital technology and surveillance tools built into our computers and smart devices translate our personal information into electronic forms and links recognizable to these systems and their distributive capacities (Gunkel, 2018). Therefore, no matter what happens inside machines or what is displayed on the screens of our smart devices, the underlying operations are stored as data after elaborate encoding and processing (Gunkel, 2018). As a result, digital data link us and our materialities to a surveillance economy in which our physical bodies and experiences enter into a technology of power that deconstructs them, analyzes them, and rearranges them semiotically and textually to create the very representations that are then used to control us using surveillance technologies inaugurated by ARPA (Dennis, 2026; Knox, 2021; Tau, 2024; Ulbricht & Egbert, 2024). This insight might explain why Jones (2020) claimed, "Surveillance has always been about the production and circulation of texts. It is not enough to monitor someone—the results of that monitoring must somehow be 'documented'" (p. 719). Based on his evaluation, Jones (2020) might agree that the acts of seeing, monitoring, and judging become central to our understanding of the textual representations and relations that documentation—in analog or digital modes—inspires (Dennis, 2024; Foucault, 1995; Peirce, 1955). Documentation and the semiology associated with the texts that it generates make the translation of surveillance and representation possible. Therefore, surveillance is never a simple or singular process because it always involves a chain of signs and actions, each with different goals and mediational means, affordances, and constraints (Jones, 2020). However, Lunceford (2018) observed, "Although we realize that the digital world is malleable, it can be difficult to make the mental adjustment to this reality when viewing the body" (p. 146). If this is the case, then it may be worth considering what parasitic pedagogy looks like as practice and governance, particularly as it pertains to the datafication of our personal information and the manifestation of our data doubles to benefit others.

Parasitic Pedagogy as Practice

A philosophical perspective on parasitic pedagogy as practice and governance involves an exploration of the material relations that underscore its constitution and protocols. As evidenced earlier in this study, data and texts are both sign systems integrated and mobilized by digitalization and computerization. To emphasize their synonymity and interchangeability, I present the datatext as the master trope that permeates parasitic pedagogy as it operates to produce the data doubles and surplus value that technology companies prize and prioritize. In other words, we might imagine a text as a system of signs or a network of unstructured data. To clarify, Benoit (2020) claimed, "Because 'data' means, in its simplest form, information collected for use, text starts to become data when we record it for reference or analysis, and this process always involves imposing some abstraction or structure that exists outside the text itself" (p. 463). Thus, I argue that parasitic pedagogy is operationalized by the character of datatexts. The interrelations that constitute datatexts also underwrite the parasitism and

semiology that govern and condition their constitution, whether they represent human (people) or nonhuman (things) entities.

Therefore, in the remaining sections of this study, I enrich our understanding of the character of datatexts in parasitic pedagogy by revealing how they mediate and govern the representation, formation, and surplus value of our nonhuman data doubles as sources and products of extractive learning—or learning based on the surveillance, extraction, cultivation, and instrumentalization of our personal data by technology companies using digital technology and internet platforms (Beck, 2015; Singh, 2017; Zuboff, 2019). First, I must explain the connection between datatexts and datafication. As the engine in the process and practice of parasitic pedagogy, datafication manifests datatexts every time digital technology, the internet, and surveillance protocols are used to extract and translate our personal information into data that produce surplus value and learning that benefits technology companies or government agencies while simultaneously constraining our agency as humans. Therefore, it is essential to clarify our conceptualization of the role of datafication in parasitic pedagogy as practice and governance.

More significantly, clarifying our appreciation of datafication helps us contextualize parasitic pedagogy based on the surveillance practices associated with technology companies. In fact, what distinguishes the digitalizing capacities of modern technology is datafication. The term is typically used to describe a form of knowledge production that transforms, reconstitutes, and rearticulates all kinds of objects, practices, behaviors, and actions into digital information or datatexts using digital machinery, communication networks, and complex infrastructures (Williamson et al., 2024). Datafication is also a principal process in the expansion of surveillance, the advancement of artificial intelligence, and the instrumentalization of algorithms and datatexts. In fact, datafication is increasingly transfiguring the cultural, political, and economic environments of the social and institutional systems it influences as we increasingly engage the world through our computers and smart devices. Therefore, it is because of datafication that datatexts become the most consequential (re)formulation of the digitalized information used to substitute and supplant material objects and the social processes they signify and govern (Benoit, 2020; Gourlay, 2021; Lamdan, 2023; Williamson et al., 2024).

As one of the most dynamic agents in the production of datatexts, humans generate information that is highly valued by technology companies and many government agencies (Tau, 2024; Zuboff, 2019). Datatexts can function as information surrogates or data doubles for humans because our data doubles reflect the accumulation of details about our identities, beliefs, and other personal information. In short, datatexts and data doubles are one and the same. With few exceptions, the accumulations or assemblages used to construct and configure these two entities are inseparable from the surveillance, probing, and tracking of people as they live and learn in their everyday lives, thus making visibility and *seeing* the key conditions in the formation, production, and representation of datatexts (Dennis, 2026; Sadowski, 2019). Thus, surveillance practices using digital technology normalize individuals by turning them into objects or data doubles whose representation can always be organized

and governed based on datatexts and their instrumentalization for the benefit of others. Williamson et al. (2020) claimed, "The datafication of human beings affects how they are understood, treated, and acted upon. The concept of the 'data double' usually refers to how digital profiles can be created from the activities of individuals" (p. 358). They added, "These profiles, or shadows, then become the basis for various forms of analysis and calculation, which circle back into individual experiences" (p. 358). The authors indicated that the creation of data doubles through datafication is inherently pedagogical. More specifically, datafication operates as a reductive pedagogy, particularly for those who might argue that only learning that can be datafied is valuable. When this view of pedagogy is imagined in the context of education, it would likely be considered problematic by most educators. However, in the boardroom of a technology company, the pedagogical reductionism that Williamson et al. (2020) associated with datafication would likely be distinguished as a capitalist imperative in which more value is placed on datatexts and data doubles than on their human counterparts (Sadowski, 2019; Zuboff, 2019). In fact, scholars have pointed out that the concept of learning—as many technology companies perceive it—may be unrecognizable to some educators. For instance, Zuboff (2019) has framed learning—as it is associated with the surveillance protocols of technology companies—in terms of surveillance and what can be operationalized from the practice of monitoring, extracting, and instrumentalizing elements such as datatexts. As people, processes, and objects are reconstituted and rearticulated as datatexts by technology companies, we are likely to continue to see competing approaches to learning as it is understood and practiced by technology companies and educators in academic systems that often depend on the technological devices, platforms, and program innovations that these companies provide (Dennis, 2025a; Higdon & Butler, 2025; Zuboff, 2019). Therefore, these companies essentially control the formulation and pedagogical expression of datatexts, their flow and surplus value, and the asymmetries of knowledge and power they generate (Demichelis, 2022; Knox, 2021; Zuboff, 2019).

Unsurprisingly, those who control datatexts are also the dominant players in parasitic pedagogy as practice and governance. For example, as a sign, the datatext is also a unit of relation between humans as data providers (hosts) and the agents or organizations (parasites) that control data extraction systems and digital processes and infrastructure. When the parasite extracts data from the host, the extracted information functions as the lifeblood that ensures the survival and growth of the parasite through its control, transformation, and instrumentalization of that information in the form of datatexts or data doubles (Patterson, 2018; Zuboff, 2019). In other words, the extractions from the host (humans) manifest the data doubles (nonhumans) that can then be exploited and commodified for the benefit of the parasite (technology companies). Therefore, datatexts and data doubles have value as a source of profit and learning, increasingly at the expense of the host. More significantly, the parasite survives by continuously feeding on information extracted from the host. In this instance, the exploitation and rearticulation of the host's material and nonmaterial resources and realities include its formal and informal learning experiences (Kim, 2022; Serres, 1982). Patterson (2018) reminded us that parasitism in any form is always a relation of power and control. In terms of the parasitic pedagogy of technology companies, parasites can exercise a disproportionate amount of control over the host and the manifestation, representation, and

instrumentalization of datatexts and data doubles. Therefore, parasitic pedagogy could be a powerful framework for contemplating and explaining the complexities of a totally pedagogised society and our different understandings of teaching and learning in formal and informal settings (Bernstein, 2001; Dennis, 2025c; Patterson, 2018, Tyler, 2004).

As a framework, parasitic pedagogy enriches our understanding of the pedagogy and learning that often occur in the digital environments between humans and nonhumans. In traditional academic settings, pedagogy typically describes a relationship between educators and learners. Learners acquire skills, experiences, and new forms of conduct from educators (Bernstein, 2000; Dennis, 2025c). Parasitic pedagogy undermines this model, particularly as it relates to networked learning and digital education (Demichelis, 2022; Dennis, 2024). More specifically, parasitic pedagogy strips away "the illusion that the networked form has some kind of indigenous moral content, that being 'connected' is somehow intrinsically pro-social, innately inclusive, or naturally tending toward the democratization of knowledge" (Zuboff, 2019, p. 9). In this study, digital technology, datafication, and the datatexts they spawn are recognized as parasitic systems and tools for pedagogic governance that feed on every aspect of our lives because they have been operationalized for the benefit of others (Dennis, 2025b; Zuboff, 2019). This insight troubles the characterization of networked learning as it is supported by organizations and advocates associated with NLEC and connectivism. Therefore, the connections, collaborations, and networks promulgated by those who support digital technology may be more exploitative, disempowering, and nonconvivial than many of us have recognized. This concern should lead us to question how effective critical or emancipatory dispositions and pedagogies would be as additional updates to the characterization of networked learning in the future (NLEC, 2021, p. 322). New paradigms and understandings of networked learning and pedagogy may need to be considered, particularly because they operate beyond the walls of academic institutions. In fact, this study suggests that the human-to-human relations and collaborations in networked learning as defined by NLEC and others would look quite different through the lens of parasitic pedagogy. With that said, this lens is useful because it helps us recognize how the surveillance practices that technology companies support also align with parasitic pedagogy as it has been conceived in this study. If this is the case, then parasitic pedagogy may be the kind of discourse and framework that we need to contemplate the role of pedagogy outside the field of education and its impact on events inside it, particularly with respect to networked learning and digital education.

Conclusion

To advance parasitic pedagogy as a form of *governance* in the Bernsteinian sense of this term, this study has revealed how the practices associated with datafication and datatexts illuminate the ways technology companies have turned the inherent parasitism and semiology in texts, data, and extractive learning into business models using digital technology, surveillance, and the internet. To encapsulate this process, parasitic pedagogy has been reimagined to help us articulate how technology companies can colonize and control human

(dis)embodiment with datatexts or data doubles, thus propagating what Bernstein (2001) imagined as the totally pedagogised society. As datatexts or information surrogates, data doubles serve as our nonhuman representations—thus granting them an alternative existence and role that technology companies can govern and assetize with limited concern about public protests, social inequality, or the kinds of upheavals that legitimized the creation of ARPANET as a pedagogical instrument. The afterlife or legacy of ARPANET lives on in the form of artificial intelligence, smart devices, and sophisticated algorithms that enable the surveillance capacities and practices that intertwine our physical bodies and data doubles in a seemingly co-dependent or parasitic relationship. As a result, technology companies and government agencies in the United States and beyond have acquired an enormous amount of power and influence over our physical bodies and behavior through the semiology and knowledge produced by our nonhuman data doubles.

In other words, our data doubles can be governed and commanded by hidden players, used to monitor our habits, and adjusted to regulate our life chances as humans (Lunceford, 2018; Williamson et al., 2020). Presently, data doubles are increasingly operationalized to exploit what is learned in formal education and elsewhere. Thus, the evidence in this study supports the claim that some of the learning goals that educators hope to achieve using networked learning and digital education are being accomplished—fundamentally but not completely—by technology companies using more sophisticated versions of the computer-aided information and surveillance technology originally developed by ARPA to combat foreign and domestic insurgencies. Our modern technology and surveillance practices emerged from the development of ARPA and ARPANET. Technology companies and others have advanced this legacy and its surveillance practices in unimaginable ways. By advancing technology, these companies also enrich our understanding of pedagogic governance using nonhuman representations or data doubles. In many ways, the approaches and practices of these companies seem to outpace those of professional educators. In fact, critics have indicated that many scholars and educators do not recognize or understand the significance of data doubles inside or outside the field of education (Bayne & Jandrić, 2017; Beck, 2015; French & Smith, 2016; Pierlejewski, 2020). Furthermore, posthumanists often argue that "most digital education practice still has not taken onboard the idea that the cyborg learner, or the online learner, or the digital learner, is a different kind of subject" (Bayne & Jandrić, 2017, p. 202). Therefore, in the future, a Bernsteinian understanding of pedagogy may be what scholars and educators need to address this issue and others that are just over the horizon (Singh, 2017; Williamson et al., 2022).

However, as we wait, an uncomfortable question remains before us. The question is, how much agency, freedom, and edification can a human expect to have when engaging a ubiquitous and technological surveillance system that was initially operationalized to combat insurgency and quell calls for social and economic equality in the United States and abroad? Whether this question is considered ontological, epistemological, or rhetorical, this study recommends parasitic pedagogy as a salient discourse and starting point for framing our responses and generating the kind of interdisciplinary awareness and dialogue that

encourages us to recognize its significance as a semiotic practice and expression of pedagogic governance used far beyond the field of education.

References

An, T., & Oliver, M. (2020). What in the world is educational technology? Rethinking the field from the perspective of the philosophy of technology. *Learning, Media and Technology*, *46*(1), 6-19.

Ball, K., & Snider, L. (Eds.). (2013). *The surveillance-industrial complex: A political economy of surveillance*. Routledge.

Bayne, S. (2024). Networked learning and utopia. *Proceedings of the International Conference on Networked Learning*, *14*(1). https://doi.org/10.54337/nlc.v14i1.8021.

Bayne, S., & Jandric, P. (2017.) From anthropocentric humanism to critical posthumanism in digital education. *Knowledge Cultures*, *5*(2), 197-216.

Beck, E. N. (2015). The invisible digital identity: Assemblages in digital networks. *Computers and Composition*, *35*, 125-140.

Beetham, H., Collier, A., Czerniewicz, L., Lamb, B., Lin, Y., Ross, J., Scott, A. M., & Wilson, A. (2022). Surveillance practices, risks and responses in the post pandemic university. *Digital Culture and Education*, *14*(1), 16-37.

Beetham, H., & Sharpe, R. (Eds.). (2020). *Rethinking pedagogy for a digital age: Principles and practices of design* (3rd ed.). Routledge.

Benoit, K. (2020). Text as data: An overview. In L. Curini & R. Franzese (Eds.), *The Sage handbook of research methods in political science and international relations* (Vol. 1, pp. 461-497). Sage.

Bernstein, B. (2000). *Pedagogy, symbolic control, and identity: Theory, research, critique* (Rev. ed.). Rowman & Littlefield.

Bernstein, B. (2001). From pedagogies to knowledges. In A. Morais, I. Neves, B. Davies, & H. Daniels (Eds.), *Towards a sociology of pedagogy: The contribution of Basil Bernstein to research* (pp. 363-368). Peter Lang.

Botz-Bornstein, T., & Stamatellos, G. (Eds.). (2022). *Parasite: A philosophical exploration*. Brill.

Cole, D. R., Bradley, J. P., & Lee, A. T. G. (2021). A pedagogy of the parasite. *Studies in Philosophy and Education*, *40*(5), 477-491.

Dammann, F., Eichenmüller, C., & Glasze, G. (2022). Geographies of "digital governmentality": Platform-based governing through adaptive environments. *Digital Geography and Society, 3*. https://doi.org/10.1016/j.diggeo.2022.100034

Demichelis, L. (2022). *Marx, alienation and techno-capitalism*. Springer.

Dennis, J. (2020). Languaging network learning: The emergence of connectivism in architectonic thought. *The International Review of Research in Open and Distributed Learning*, *21*(3), 304-318.

Dennis, J. (2024). Slavery's afterlife in Black education: Foucauldian architectonics and the discourse of racial surveillance and pedagogy. *Journal of African American Studies*, *28*(2), 136-153. https://doi.org/10.1007/s12111-024-09663-8

Dennis, J. (2025a). Postmodern paradox: Artificial intelligence, pedagogy and the return of

robot slavery. *Journal of Contemporary Issues in Education, 20*(1), 293-322.
Dennis, J. (2025b). Surveillance education: Silence and slavery in pedagogical discourse. *Critical Questions in Education, 16*(2), 179-197.
Dennis, J. (2025c). Toni Morrison's *Beloved*: Plantations, pedagogy and the future of digital slavery. *Journal of Interdisciplinary Sciences, 9*(1), 63-84.
Dennis, J. (2026). Policing Black data: The semiology of carcerality and slavery in Michel Foucault's *Discipline and Punish*. *Race and Justice, 16*(2), 646-671. https://doi.org/10.1177/21533687251377229
Downes, S. (2019). Recent work in connectivism. *European Journal of Open, Distance and E-Learning, 22*(2), 113-132.
Foucault, M. (1995). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage Books.
Foucault, M. (2000). Governmentality. In J. D. Faubion (Ed.), *Power* (pp. 201-222). The New Press.
French, M., & Smith, G. J. (2016). Surveillance and embodiment: Dispositifs of capture. *Body & Society, 22*(2), 3-27.
Gilliard, C., & Selwyn, N. (2023). Automated surveillance in education. *Postdigital Science and Education, 5*(1), 195-205.
Giroux, H. A. (2004). Cultural studies, public pedagogy, and the responsibility of intellectuals. *Communication and Critical/Cultural Studies, 1*(1), 59-79.
Giroux, H. A. (2015). Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies, 29*(2), 108-140.
Gourlay, L. (2021). *Posthumanism and the digital university: Texts, bodies and materialities*. Bloomsbury.
Gunkel, D. J. (2018). Critique of digital reason. In A. Hess & A. Davisson (Eds.), *Theorizing digital rhetoric* (pp. 19-31). Routledge.
Higdon, N., & Butler, A. (2025). *Surveillance education: Navigating the conspicuous absence of privacy in schools*. Routledge.
Hinchliffe, G. (2001). Education or pedagogy? *Journal of philosophy of education, 35*(1), 31-45.
Irvine, M. (2023). Semiotics in computing and information systems. In J. Pelkey & S. W. Matthews (Eds.), *Semiotics in the natural and technical sciences* (Vol. 2., pp. 203-237). Bloomsbury Publishing.
Jacobsen, A. (2015). *The Pentagon's brain: An uncensored history of DARPA, America's top-secret military research agency*. Little, Brown and Company.
Jones, R. (2020). Discourse analysis and digital surveillance. In A. De Fina & A. Georgakopoulou (Eds.), *The Cambridge handbook of discourse studies* (pp. 708-731). Cambridge University Press.
Karp, A., & Zamiska, N. W. (2025). *The technological republic: Hard power, soft belief, and the future of the West*. Crown Currency.
Kim, H. K. (2022). The parasite is the truth of the system. In T. Botz-Bornstein & G. Stamatellos (Eds.), *Parasite: A philosophical exploration* (Vol. 377., pp. 157-169). Brill.

Kitchin, R. (2021). *Data lives: How data are made and shape our world*. Bristol University Press.

Knox, J. (2021). Refocusing Zuboff's 'division of learning' on education. *Seminar.net: International Journal of Media, Technology & Lifelong Learning, 17*(2). https://doi.org/10.7577/seminar.4268

Lamdan, S. (2023). *Data cartels: The companies that control and monopolize our information*. Stanford University Press.

Land, R., & Bayne, S. (2005). Screen or monitor? Issues of surveillance and disciplinary power in online learning environments. In R. Land & S. Bayne (Eds.), *Education in cyberspace* (pp. 165-178). Routledge.

Landow, G. P. (2006). *Hypertext 3.0: Critical theory and new media in an era of globalization*. The Johns Hopkins University Press.

Levine, Y. (2018). *Surveillance valley: The secret military history of the Internet*. PublicAffairs.

Lewin, D., & Lundie, D. (2016). Philosophies of digital pedagogy. *Studies in Philosophy and Education, 35*, 235-240.

Lunceford, B. (2018). Where is the body in digital rhetoric? In A. Hess & A. Davisson (Eds.), *Theorizing digital rhetoric* (pp. 140-152). Routledge.

Lyon, D. (1994). *The electronic eye: The rise of the surveillance society*. University of Minnesota Press.

Lyon, D. (2022). Reflections on forty years of "surveillance studies". *Surveillance & Society, 20*(4), 353-356.

Monahan, T., & Torres, R. D. (2010). *Schools under surveillance: Cultures of control in public education*. Rutgers University Press.

Nemorin, S. (2017). Post-panoptic pedagogies: The changing nature of school surveillance in the digital age. *Surveillance & Society, 15*(2), 239-253.

Networked Learning Editorial Collective (2021). Networked learning: Inviting redefinition. *Postdigital Science and Education, 3*, 312-325.

O'Mara, M. (2019). *The code: Silicon Valley and the remaking of America*. Penguin.

Patterson, O. (2018). *Slavery and social death: A comparative study*. Harvard University Press.

Peirce, C. S. (1955). *Philosophical writings of Peirce* (J. Buchler, Ed.). Dover.

Peters, M. A. (2023). Digital trade, digital economy and the digital economy partnership agreement (DEPA). *Educational Philosophy and Theory, 55*(7), 747-755.

Pierlejewski, M. (2020). The data-doppelganger and the cyborg-self: Theorising the datafication of education. *Pedagogy, Culture & Society, 28*(3), 463-475.

Ravenscroft, A. (2011). Dialogue and connectivism: A new approach to understanding and promoting dialogue-rich networked learning. *International Review of Research in Open and Distributed Learning,12*(3), 139-160.

Ross, J. (2023). *For learning: Speculative methods and pedagogies*. Routledge.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society, 6*(1), 1-12.

Schick, K., & Timperley, C. (Eds.). (2022). *Subversive pedagogies: Radical possibility in the academy*. Routledge.

Sefton-Green, J. (2022). Towards platform pedagogies: Why thinking about digital platforms as pedagogic devices might be useful. *Discourse: Studies in the Cultural Politics of Education, 43*(6), 899-911.

Semetsky, I. (Ed.). (2017). *Edusemiotics: A handbook*. Springer.

Serres, M. (1982). *The parasite* (Vol. 1). University of Minnesota Press.

Siemens, G. (2017). Connectivism: A learning theory for the digital age. In R. E. West (Ed.), *Foundations of learning and instructional design technology*. https://pressbooks.pub/lidtfoundations/chapter/connectivism-a-learning-theory-for-the-digital-age/

Singh, P. (2017). Pedagogic governance: Theorising with/after Bernstein. *British Journal of Sociology of Education, 38*(2), 144-163.

Tau, B. (2024). *Means of control: How the hidden alliance of tech and government is creating a new American surveillance state*. Crown.

Tyler, W. (2004). Silent, invisible, total: Pedagogic discourse and the age of information. In J. Muller, B. Davies, & A. Morais (Eds.), *Reading Bernstein, researching Bernstein* (pp. 15-29). Routledge.

Ulbricht, L., & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society, 11*(3). https://doi.org/10.1177/20539517241255108

Williamson, B., Bayne, S., & Shay, S. (2020). The datafication of teaching in higher education: Critical issues and perspectives. *Teaching in Higher Education, 25*(4), 351-365.

Williamson, B., Gulson, K. N., Perrotta, C., & Witzenberger, K. (2022). Amazon and the new global connective architectures of education governance. *Harvard Educational Review, 92*(2), 231-256.

Williamson, B., Komljenovic, J., & Gulson, K. (Eds.). (2024). *World yearbook of education 2024: Digitalisation of education in the era of algorithms, automation and artificial intelligence*. Routledge.

Zou, Y., Kuek, F., Feng, W., & Cheng, X. (2025). Digital learning in the 21st century: Trends, challenges, and innovations in technology integration. *Frontiers in Education, 10*. https://doi.org/10.3389/feduc.2025.1562391

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs/Hachette.

Paper Received March 8, 2026; Accepted April 6, 2026; Published May 2, 2026