Secrecy and Society

ISSN: 2377-6188

Volume 1
Number 2 *Secrecy and Authoritarianism*

Article 5

February 2018

Secrecy in Educational Practices: Enacting Nested Black Boxes in Cheating and Deception Detection Systems

Jo Ann Oravec
University of Wisconsin - Whitewater, oravecj@uww.edu

Secrecy in Educational Practices: Enacting Nested Black Boxes in Cheating and Deception Detection Systems

Abstract

This paper covers secrecy from the vantage point of recent technological initiatives designed to detect cheating and deception in educational contexts as well as to monitor off-campus social media speech code violations. Many of these systems are developed and implemented by third-party corporate entities who claim practices to be proprietary and secret. The outsourcers involved in these efforts have provided one level of secrecy and educational administrators involved yet another level, thus constructing "nested black boxes." Also discussed in this paper is the “paranoid style” of administration, often supported by the surveillance and construction of rosters of potential non-conformists, such as alleged cheaters and speech code violators. The educational technologies described in this article are increasingly applied to workplace practices, with young people being trained in what is deemed acceptable conduct. Secrecy can serve to alter the character of relationships within the educational institutions involved as well as inside the workplaces in which the approaches are increasingly being integrated.

Keywords

black boxes, cheating detection, deception, educational institutions, Richard Hofstadter, machine learning, outsourcing, paranoid style, secrecy, secrecy studies

Creative Commons License

Secrecy in Educational Practices: Enacting Nested Black Boxes in Cheating and Deception Detection Systems

Abstract

This paper covers secrecy from the vantage point of recent technological initiatives designed to detect cheating and deception in educational contexts as well as to monitor off-campus social media speech code violations. Many of these systems are developed and implemented by third-party corporate entities who claim practices to be proprietary and secret. The outsourcers involved in these efforts have provided one level of secrecy and educational administrators involved yet another level, thus constructing "nested black boxes." Also discussed in this paper is the “paranoid style” of administration, often supported by the surveillance and construction of rosters of potential non-conformists, such as alleged cheaters and speech code violators. The educational technologies described in this article are increasingly applied to workplace practices, with young people being trained in what is deemed acceptable conduct. Secrecy can serve to alter the character of relationships within the educational institutions involved as well as inside the workplaces in which the approaches are increasingly being integrated.

Keywords: black boxes, cheating detection, deception, educational institutions, Richard Hofstadter, machine learning, outsourcing, paranoid style, secrecy, secrecy studies

Educational institutions play vital roles in conveying to future generations various expectations for how organizations operate and how individuals are construed as human beings. This article discusses secrecy issues in cheating and deception detection initiatives as well as the off-campus social media monitoring of students, emphasizing their socially negative and organizationally dysfunctional aspects. It uses the notions of "black boxes" (Ashby 1961; Glanville 1982) and "paranoid style" (Hofstadter 2012; Wamsley, Schroeder, and Lane 1996) to underscore secrecy-related dimensions in educational settings. The implications of a charge of cheating or of online speech violations can be significant if not debilitating for students and their households, giving these issues special urgency; a "false positive" system result could be overwhelming to the individuals who are under suspicion, resulting in anxiety and diminished reputation. The developers and implementers of the systems discussed in this article are often corporations that serve as outsourcers for critical educational functions (including Verificient Technologies, Inc. and ProctorU, Inc.), rather than educational institutions themselves. Their various interactions with educational institutions are often not easily accessible; this can make efforts to map extents and levels of secrecy difficult.

This article extends black box analyses in light of the multiple, intersecting entities involved in cheating detection. Black boxes contain algorithms and operations inaccessible to the users and observers of the boxes' operations, who generally view only inputs and outputs. Many of the conceptual underpinnings for black box approaches were formulated in the context of military initiatives during and soon after World War II, initiatives that often involved levels of complexity that few people could decipher and even fewer could control. Black box concepts soon permeated the thinking of many varieties of system designers and researchers (Von Hilgers 2011). In the “nested black box” formulation, secrecy can be a critical factor both at the levels of system programming (the algorithms involved) and of administrative system utilization.

For the technological applications discussed in this article, the institutional rationales for secrecy of basic system operations often include the potentials for inappropriate exposure of proprietary information of the outsourcers who developed the system, a common approach in supporting the protection of corporate information in high tech systems (Vedder and Naudts 2017). According to the logic of such secrecy, if the algorithms and techniques associated with the systems would be widely available the developers could not obtain appropriate compensation for their creative efforts. Other rationales for secrecy are sometimes presented by system implementers: for example, in particular cheating detection systems, exposure of some system operations may supposedly damage the systems’ capabilities for identifying cheaters. The logic behind these concerns includes that with increased levels of system knowledge individuals could learn how to “game” the systems and share these insights with others.

The shame and societal stigmas of being associated with cheating in educational contexts may serve to stifle some efforts to investigate the systems involved. For example, even exposing the number of false positives generated can serve to embarrass and demoralize individuals involved in the system. Educational institutions serve as fertile development sites for new approaches for cheating and deception detection, often with little open opposition by participants; the kinds of technologies integrated into such detection are being exported to other arenas, with some workplace monitoring systems already produced and maintained by Verificient Technologies, Inc. and ProctorFree, Inc.

Technical and Legal Dimensions of Educational Secrecy

Secrecy of some form is part of a number of traditional educational practices and social groupings, including secret campus societies (Creech 2008). Although most students may not have been under the threat of “double secret probation” as portrayed in the 1978 US film *Animal House* (Universal Pictures), they are often given evaluation experiences that involve the withholding of information. Secrecy involves a form of power on the part of the secret holders, which can relate to professional and expertise-related attainment as well as societal status. As described in Maret (2016), secrecy in organizational contexts can leverage access to information and be considered as a “tampering of communications” in Friedrich’s (1972) perspective.

The black box aspects of the systems described in this article can have problematic implications in educational contexts. The notion of the black box has a long history in thinking about systems (Glanville 1982). Technological and administrative black boxes can work in distinct ways as well as interact with each other; assertions by supposed experts about the complexity involved in the technologies can add rhetorical dimensions to the secrecy issues involved in both the applicable technical and administrative dimensions. For example, black box systems rooted in proprietary and secret algorithms can be nested within administrative structures that are themselves opaque in terms of the specifics of the algorithms' applications. Ashby (1961) and some other researchers who have developed black box notions have projected that black boxes are widespread phenomena rather than restricted or isolated entities (Bucher 2016), with their numbers and varieties increasing with expansions in the societal utilization of technical systems. Developers and implementers may provide the rationale that the systems are too intricate to be understood by certain audiences; in some recent cases, "machine learning" algorithms and other artificial intelligence (AI) approaches have been considered too complex for explanation to non-technical audiences (Sandvig 2014).

The notion that secrecy is an acceptable part of some common educational practices is widespread. For centuries, exams have been given with some level of secrecy in order to encourage students to prepare and be evaluated in ways that are supposedly designed to accommodate fairness. Education, on the other hand, is widely associated with openness and clarity as individuals are introduced to various concepts and supposedly evaluated in a manner that is largely transparent. For instance, proctors or invigilates in many face-to-face testing settings generally apply transparent examination rules in physical environments open to some level of external observation by participants. However, "high stakes" testing has introduced a number of outsourcer-related secrecy issues to education in the US, UK, and other nations. Tests designed and implemented by third-party organizations are often construed in legal and public policy contexts as forming a positive societal good, and legal and activist efforts to counter these systems are often futile. The proprietary nature of some of the systems introduced into education at various levels can increase the distance between households and the educational systems that support their students' development and societal advancement. The Family Educational Rights and Privacy Act (FERPA), originally enacted in 1974, had served to protect student data in terms of household privacy and access rights (Oravec 2003). However, amendments in 2014 diminished these protections, expanding corporate outsourcer access and control opportunities:

> Recent amendments to FERPA expanded the circle of parties with which student data can be shared. Not only are the companies providing learning data systems often not clear about with whom they share data, parents are concerned about what will eventually come of behavioral data and other assessments—and whether that information will permanently limit their child's future. (Miller 2014, 112)

An increasingly wide range of everyday educational activities have incorporated secret practices in part because of technological shifts that supposedly require the involvement of outsourcers, including the use of security consultants and the installation and operation of school surveillance cameras (Baporikar 2017; Perry-Hazan and Birnhack 2016). Students and other stakeholders in educational systems are often not allowed to access specific information about practices that are conducted by educational outsourcers; their off-campus exchanges of information can be monitored as well. They are thus not equipped to learn more details about the practices or be able to determine whether various discriminatory dimensions are involved. The expansions of surveillance along with increased emphases on metrics-centered evaluation at many levels in educational systems have opened critical questions concerning the basic relationships among the institutions' participants (Oravec 2017; Samier 2014; Shade and Singh; Taylor 2013). In the U.S. educational context, Reys (2016) decried the encroachment of proprietary influences in the realm of testing by stating "Too Much Testing, Too Little Control, Transparency Needed."

The legal contexts of testing and educational practices in the U.S. and UK provide some clues as to why secrecy is often considered acceptable in educational practices. Educational testing organizations in the U.S. and UK have often been given only limited restrictions on what they can do in their efforts to create credible and economically lucrative testing systems. For example, the Educational Testing Service (ETS) has generally been supported in its attempts to invalidate test scores of individuals deemed to be cheating in some way; in plagiarism detection efforts, the Turnitin organization has also successfully fought hundreds of legal attacks for its apparent usurpation of student copyrights and other supposed affronts (Muriel-Torrado and Fernández-Molina 2015). Corporations have often served as outsourcers for many educational functions that involve critical technical dimensions; this arrangement can serve to deflect some of the concern that inherent system biases and deficiencies could be exposed and the relevant educational administrations put at risk.

Big Data and Cheating Detection Systems

Research and development efforts on educational deception have acquired new dimensions in the advent of big data capabilities, often adding complexities to the black boxes involved. Insights from data analytics and machine learning are increasingly incorporated into efforts involving cheating in online education and evaluation. Comparable approaches are being used to predict and detect deception in business and community safety contexts (Blair, Levine, and Vasquez 2015). Constructions of “integrity scores” rooted in the operation of proprietary, secret algorithms make it possible for opportunistic selection of which potential cheaters to target. These practices can place students in a disempowered, asymmetrical position; the difficulties in defending against allegations of cheating by a big data-enhanced system could diminish the position of the student as a moral agent. Consider the following example from the *New York Times* of the use of such systems in higher education:

> Before Betsy Chao, a senior here at Rutgers University, could take midterm exams in her online courses this semester, her instructors sent emails directing students to download Proctor track [from Verificient Technology], a new anti-cheating technology. "You have to put your face up to it and you put your knuckles up to it," Ms. Chao said recently, explaining how the program uses webcams to scan students' features and verify their identities before the test. Once her exam started, Ms. Chao said, a red warning band appeared on the computer screen indicating that Proctor track was monitoring her computer and recording video of her. To constantly remind her that she was being watched, the program also showed a live image of her in miniature on her screen. (Singer 2015, B-1)

Muñoz (2015) and others describe the integrity scores that are compiled about test takers' levels of compliance as being based on algorithms that are proprietary to the outsourcers involved.

Utilization of these technologically-enabled approaches for identifying potential cheaters and bullies is especially legally and ethically problematic with children, but can also affect the lives of the adults and households involved. Many individuals are being surveilled from birth with technologies that include crib monitors and interactive toys (Marx and Steeves 2010; Oravec 2000). They are also increasingly learning through their interactions with deception detection systems and related educational technologies what the systems construe as "acceptable" in terms of their potential of engaging in non-conformist behavior. Educational administrators, teachers, and parents are often provided by the systems with information involving children's propensity to cheat (including the previously-mentioned integrity scores) that is difficult to interpret in practical terms. Other deception-related situations (such as border control) involve comparable approaches, and technological developments that are rooted in these initiatives are likely to be applied in educational contexts at some point.

Social media monitoring of students' off-campus interactions can also involve secret, proprietary algorithms and related systems:

> There are other examples where school officials have overreacted to undesirable student speech that reflects nothing more than routine dissension and general dissatisfaction with school personnel. One notable example involves a twelve year-old sixth grader who was disciplined for posting on her Facebook website that she "hated" an adult hall monitor because the aide was "mean" to her." The message, posted from a home computer after school hours, was shown to the school principal by another student and the girl was disciplined for bullying. The student subsequently posted a second message on her Facebook page saying that she wanted to know the identity of the student who told the principal about her posting, and in response to this second message, the student received an in-school suspension and was also prohibited from attending a class ski trip. (Sheridan 2015, 63)

The students and households who face administrative scrutiny concerning the appropriateness of off-campus social media postings would want information about how these postings were selected such as what criteria were used to flag these messages? Being labeled as an online "bully" or speech code violator could be devastating to students. However, given the proprietary nature of the third-party outsourcer that developed and implemented the system involved, specific algorithmic characterizations were not forthcoming, providing a "nested" black box. The logic that such details about the algorithms could be used to circumvent the systems' gaze is also characteristic of the institutional discourse supporting secrecy.

Experimentation issues in system development provide another dimension to secrecy concerns in education. The organizations that are attempting to develop new forms of surveillance and behavioral analysis may certainly choose to engage in some levels of testing and experimentation on aspects of their systems with students in live situations, even though these initiatives may have a negative impact on some of the subjects involved. If the secrecy about the effort ends and the nature of the experimentation is exposed, subjects may certainly leave the experiment, deflating its value for experimenters.

Ramifications for Students, Households, Educators, and System Developers

As previously stated, the social consequences of being labeled as potential "cheaters" or online "bullies" in an official compilation of individuals' names may be devastating to those listed, whether or not these lists are held with some level of security. Conscientious attention to the social and ethical issues involved is thus imperative for system developers and implementers (Majeed, Baadel, and Haq 2017; Taylor 2013). Constructions of cheating can differ among systems, possibly resulting in anxieties and cognitive dissonance in subjects (often young children) as well as confusions for individuals called upon to interpret the data produced. Some of the facial expressions and various gestures associated with deception are linked to intimate personal expressions involving thought processes (Verplaetse, Vanneste, and Braeckman 2007). Influencing these expressions could lead to disruption of the subjects' moral consideration of the situations at hand. Questions about educational applications of these technologies include considerations of whether minors as subjects (with their relative malleability) should be given particular protection.

Secrecy concerns also have significant ramifications for faculty members and administrators. Educators have obtained professional statuses in part because of their ability to control information, either the research information involved in their investigations or the teaching-related information related to evaluation of students and higher education personnel. Efforts to make some information about basic educational processes secret and inaccessible can foster the formation of tiers of educational personnel as well as increased control by external corporations. Participants in the corporations involved with the systems also play considerable moral roles and face ramifications for their actions: many high tech organizations have ethical standards and mottos that attempt to engage their participants in asking questions about the impacts of technologies (Oravec 2014). Developers of cheating-detection and social media monitoring approaches are generally third-party organizations (often startups) not directly affiliated with educational institutions, the latter which are generally bound by specific privacy and children's welfare constraints. Their long-term liability for the welfare of the students, households, and communities they affect is marginal in relation to that of the educational institutions involved.

Prospects and Long-term Impacts of Cheating-Detection and Social Media Monitoring Systems

The futures of cheating detection initiatives along with social media monitoring efforts present unsettling prospects as they are coupled with big data methodologies. Secret lists of subjects who are construed as potential cheaters or bullies could readily be compiled with the integrity scores and social media monitoring data with lifelong implications for the individuals involved. The "paranoid style" of administration can be fostered by the existence of lists of individuals who could potentially cheat, deceive, or otherwise not be in conformance with administrators, whether or not the individuals on the list are indeed exhibiting resistance or non-conformist behaviors. Individualized anti-cheating and monitoring systems linked with user profiles are also problematic. For instance, some kinds of research currently being done on deception integrate detailed information about individuals' biometric indicators and other personalized data in search of individualized patterns of signals about their deception-related intensions (Miller 2014; Hope 2016). These data may be stored and used over time as ways to ascertain whether the individuals are conforming to particular standards of integrity in various contexts. Proving conclusively that an individual is a cheater or deceiver is not possible, which adds inherent difficulties with the systems; extracted or voluntary confessions are a major mode of discovery of deception in many arenas.

The kinds of systems described in this article could have long-term impacts on subjects’ ethical thinking and related behavioral expression, as well as considerable cultural implications. The crowdsourcings of subjects’ reflections about some of the cheating-detection systems already in place are already being used by students to alter their behavior in various testing and evaluation contexts. If individuals are given little or no feedback as to what kinds of “tells” or “leakages” supposedly signal their current or planned deceptions they could minimize or exaggerate certain emotional responses or engage in the kinds of expressive repertoire recommended by others in crowdsourced comments. Also troubling are prospects for secret experimentation with the systems on the part of the researchers, developers, and implementers involved. For example, experimenters could provide false feedback to subjects with the aim of testing the systems or enhancing subjects’ responses. Systematic, machine-monitored rewarding of inauthentic responses over time based on secret criteria can present unsettling prospects for mental health as well as societal norms.

Some Conclusions and Reflections

Technological shifts in how anti-cheating and social media monitoring systems are designed and implemented are likely as new developers and methodologies emerge, creating a moving target for those concerned about educational secrecy. For individuals who wish to counter these systems through legal or public policy-related pressures, the changing technological forms as well as ownership statuses of the systems involved can put frustrating barriers in the way of modification and reform. Social shifts are likely as well. The expansion of "arms races" involving anti-cheating and social media monitoring technologies is already occurring as individuals find and share various ways to manipulate and alter their perceived identities, locations, and behaviors (Sengupta 2013; Zhao and Sui 2017). Various forms of strategic resistance by participants, whether or not supported with technology, can also be factors in how the practices will evolve (Oravec 2017; Warren 2017). Such efforts to counter and protest perceived technological intrusions have had sustained impact on the overall direction of technological development, with various surveillance mechanisms serving as challenges to talented and persistent individuals. For example, resistance to the *ProctorU* online test monitoring system in 2015 at Rutgers University resulted in development of the option for students of requesting human-conducted proctoring at an additional fee (Singer 2015). In the paranoid style formulation, the lists of potential cheaters compiled through technological methodologies can provide a form of support for administrative sanctions and other negative actions whether or not the listed individuals are indeed appropriately linked to cheating, deception, or other problematic efforts.

As previously stated, this paper emphasizes the negative dimensions of secrecy related to the black box systems. The technological initiatives described in this article are being evaluated from an assortment of perspectives and standards. **F**or example, Majeed, Baadel, and Haq (2017) contend that these initiatives can either be considered as "global triumph" or as "exploitation" as societal norms adjust to rapid changes in information and communications technology. Sandvig (2014) describes the kinds of rhetorical support that some algorithms are being given by their developers and implementers as a form of "celebrity," which serves to defend algorithm utilization in specific real-world contexts without examining relevant assumptions and underpinnings. Although the shame and other societal stigmas associated with cheating and deception may indeed be considerable, efforts to "reverse engineer" the nested black boxes and expose their potential implications may eventually serve to mitigate some of the negative effects of educational secrecy.

References

Ashby, W. Ross. 1961. *An introduction to cybernetics*. London: Chapman & Hall Ltd.

Baporikar, Neeta. 2017. Institutionalizing academic integrity: The present need. In *Handbook of research on academic misconduct in higher education*, 60-80. Hershey, PA: IGI Global.

Blair, J. Pete, Timothy R. Levine, and Bob E. Vasquez. 2015. Producing deception detection expertise. *Policing: An International Journal of Police Strategies & Management* 38, no. 1: 71-85.

Bridges, David. 2017. Research for sale? Epistemic, moral, and political drift through the commodification of educational research. In *Philosophy in educational research*, 315-339. New York: Springer International Publishing.

Bucher, Taina. 2016. Neither black nor box: Ways of knowing algorithms. In *Innovative methods in media and communication research*, 81-98. New York: Springer International Publishing.

Creech, Russell. (ed.). 2008. *Secrecy, spirituality, and political education at Princeton: The early 19th century.* Russell Creech Publisher.

Friedrich, Carl Joachim. 1972. *The pathology of politics: Violence, betrayal, corruption, secrecy, and propaganda*. New York: Harper & Row.

Hofstadter, Richard. 2012. *The paranoid style in American politics*. New York: Vintage.

Hope, Andrew. 2016. Biopower and school surveillance technologies 2.0. *British Journal of Sociology of Education* 37, no. 7: 885-904.

Majeed, Asim, Said Baadel, and Anwar Ul Haq. 2017. Global triumph or exploitation of security and privacy concerns in e-learning systems. In *International Conference on Global Security, Safety, and Sustainability*, 351-363. New York: Springer.

Maret, Susan. 2016. The charm of secrecy: Secrecy and society as secrecy studies. *Secrecy and Society* 1, no. 1: 1-28.

Marx, Gary, and Valerie Steeves. 2010. From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society* 7. no. 3/4: 192-230.

Miller, Kevin. 2014. Total surveillance, big data, and predictive crime technology: Privacy's perfect storm. *Journal of Technology, Law & Policy* 19: 105-146.

Muñoz, Daniel. 2015. ProctorTrack company releases statement on status of student data. *New Brunswick Today,* September 18. http://newbrunswicktoday.com/article/proctortrack-company-releases-statement-status-student-data

Muriel-Torrado, Enrique, and Juan-Carlos Fernández-Molina. 2015. Creation and use of intellectual works in the academic environment: Students' knowledge about copyright and copyleft. *The Journal of Academic Librarianship* 41, no. 4: 441-448.

Oravec, Jo Ann. 2000. Interactive toys and children's education: Strategies for educators and parents. *Childhood Education* 77, no. 2: 81-85.

___. 2003. The Transformation of privacy and anonymity: Beyond the right to be let alone. *Sociological Imagination* 39, no. 1: 3-23.

___. 2014. Mottos and ethical statements of Internet-based organizations: Implications for corporate social responsibility. *International Journal of Civic Engagement and Social Change* 1, no.2: 37-53.

___. 2017. The manipulation of scholarly rating and measurement systems: Constructing excellence in an era of academic stardom. *Teaching in Higher Education* 22, no. 4: 423-436.

Perry-Hazan, Lotem, and Michael Birnhack. 2016. Privacy, CCTV, and school surveillance in the shadow of imagined law. *Law & Society Review* 50, no. 2: 415-449.

Reys, Robert. 2016. Too much testing, Too little control, transparency needed. *Mathematics Teacher* 109, no. 6: 408-410.

Samier, Eugenie A. 2014. *Secrecy and tradecraft in educational administration: The covert side of educational life*. New York: Routledge.

Sandvig, Christian. 2014. Seeing the sort: The aesthetic and industrial defense of "the algorithm." *Journal of the New Media Caucus* 10, no. 3: 31-54.

Sengupta, Somini. 2013. Warily, schools watch students on the Internet. *The New York Times,* October 28. http://www.nytimes.com/2013/10/29/technology/some-schools-extend-surveillance-of-students-beyond-campus.html

Shade, Leslie Regan, and Rianka Singh. 2016. "Honestly, We're Not Spying on Kids": School surveillance of young people's social media. *Social Media + Society* 2, no. 4. doi:2056305116680005

Sheridan, Patricia M. 2015. Tracking off-campus speech: Can public schools monitor students' social media? *Southern Law Journal* 25, no.1: 57-76.

Singer, Natasha. 2015. April 6. Online test-takers feel software's uneasy glare. *The New York Times*, April 5. https://www.nytimes.com/2015/04/06/technology/online-test-takers-feel-anti-cheating-softwares-uneasy-glare.html

Taylor, Emmeline. 2013. *Surveillance schools: Security, discipline and control in contemporary education*. New York: Springer.

Vedder, Anton, and Laurens Naudts. 2017. Accountability for the use of algorithms in a big data environment. *International Review of Law, Computers & Technology* 31, no. 2: 1-19.

Verplaetse, Jan, Sven Vanneste, and Johan Braeckman. 2007. You can judge a book by its cover, the sequel: A kernel of truth in predictive cheating detection. *Evolution and Human Behavior* 28, no. 4: 260-271.

Von Hilgers, Philipp. 2011. The history of the black box: The clash of a thing and its concept. *Cultural Politics* 7, no. 1: 41-58.

Wamsley, Gary L., Aaron D. Schroeder, and Larry M. Lane. 1996. To politicize is not to control: The pathologies of control in federal emergency management. *The American Review of Public Administration* 26, no. 3: 263-285.

Warren, Simon. 2017. Struggling for visibility in higher education: Caught between neoliberalism "out there" and "in here" – an autoethnographic account. *Journal of Education Policy* 32, no. 2: 127-140.

Zhao, Bo, and Daniel Z. Sui. 2017. True lies in geospatial big data: Detecting location spoofing in social media. *Annals of GIS* 23, no. 1: 1-14.