




Facial recognition technology in schools: critical questions and concerns

Mark Andrejevic^a and Neil Selwyn ^b

^aSchool of Media, Film & Journalism, Monash University, Melbourne, Australia; ^bFaculty of Education, Monash University, Melbourne, Australia

ABSTRACT

Facial recognition technology is now being introduced across various aspects of public life. This includes the burgeoning integration of facial recognition and facial detection into compulsory schooling to address issues such as campus security, automated registration and student emotion detection. So far, these technologies have largely been seen as routine additions to school systems with already extensive cultures of monitoring and surveillance. While critical commentators are beginning to question the pedagogical limitations of facially driven learning, other this article contends that school-based facial recognition presents a number of other social challenges and concerns that merit specific attention. This includes the likelihood of facial recognition technology altering the nature of schools and schooling along divisive, authoritarian and oppressive lines. Against this background, the article considers whether or not a valid case can ever be made for allowing this form of technology in schools.

ARTICLE HISTORY

Received 2 July 2019
Accepted 22 October 2019

KEYWORDS

Biometrics; facial recognition; smart cameras; schools; surveillance

Introduction

The past few years have seen the implementation of automated facial recognition systems across a range of social realms. While these technologies are associated most frequently with promises to strengthen public safety, a growing number of other applications have also emerged – from verifying the identity of bank users, through to ‘smart billboards’ that display advertisements in response to the moods of passers-by. Of particular interest is how facial recognition technologies are beginning to be implemented in school settings. Indeed, there are now various educational applications of facial recognition and facial detection – including campus security systems, automated roll-calls and student emotion and attention monitoring. In countries such as the US, UK and Australia, these technologies have so far prompted little controversy or push-back. After all, schools in these countries have long utilised video camera surveillance systems and other forms of technology-based tracking and monitoring.

In this sense, facial recognition could be seen as a logical extension of technology-based surveillance trends established in schools from the 1990s onwards. However, in this article, we seek to problematise the specific connotations and possible consequences of facial recognition technology in schools. Drawing on emerging debates amongst communications, media and surveillance scholars, the article addresses a number of specific social challenges and concerns – not least various ways in which this technology might alter the nature of schools and schooling along divisive, authoritarian

CONTACT Neil Selwyn  neil.selwyn@monash.edu

© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

and oppressive lines. In light of recent calls from some commentators and activists for the outright banning of facial recognition in other areas of society, this paper considers whether (or not) these surveillance and monitoring technologies can ever be implemented in schools in ways that are not harmful and/or genuinely beneficial.

The emergence of facial recognition technology across society

The recent rise of facial recognition stems from parallel advances in computer vision processing (where machine learning techniques can be applied to recognise and learn from patterns in digital image data streams), alongside improvements in digital video camera technology. In simple terms, facial recognition technologies work by computationally extracting facial features captured on a digital video image, and then comparing this data with previously analysed faces already stored on a database. Crucially, these databases contain large numbers of photographed faces with associated names and other personally identifiable information.

More specifically, these systems tend to work by computationally analysing facial shapes and features in terms of the positioning and distancing between sets of geometric coordinates (for example, the centre of each pupil, the bridge of a nose, the ends of an eyebrow). Given the unique nature of every person's 'face-print', when the geometric properties of a captured image are compared against a database of pre-existing personally identifiable images the system should be able to make a match with a specific individual. Alongside this capacity to verify identities, corresponding forms of 'facial detection' technologies are being developed to scan and analyse facial expressions in order to infer people's moods, emotions and affective states.

These developments constitute a form of biometric technology – relying on measurements of human bodily characteristics in a manner similar to iris recognition, gait identification and fingerprinting. While less accurate than most other biometric methods (for example, the accuracy of digital facial imaging continues to be hampered by poor light and shadowing), facial recognition technologies retain the advantage of not requiring individuals to present themselves for inspection. This allows for the mass monitoring of large groups of people on a continuous basis. In addition, the increasing image quality of cameras in consumer electronics (such as laptops and smartphones) has enabled the expansion of relatively cheap software and apps offering device-based facial recognition.

Countries such as the US, UK and Australia are now seeing facial recognition technologies being installed and operated in a number of different types of (quasi)public space – including factories, cafes, airports, shopping areas, and government buildings. More often than not, the underlying aim of such systems is to identify and/or recognise people and track their movements. The specific applications of this technology are diverse. For example, retail providers are working on the development of pay-by-face technology. In other sectors, facial recognition technology is already being used by cafes to identify repeat customers and their regular orders (Bolger 2018). Workplaces are adopting facial recognition to allow employees to clock in and out, while airports are screening travellers by matching face scans to online images, watch lists, criminal databases and social media (Burt 2018). Perhaps most contentiously, cameras equipped with facial recognition technology are now being used by law enforcement agencies to identify criminals and search for missing persons (Grubb 2018).

Alongside these personal identification techniques, are systems based around principles of facial detection (where faces are scanned but not matched to particular individuals). For example, such technology is now being used to read expressions and track de-identified individuals from the camera to camera across shopping malls with the intention of inferring the gender, age, and 'mood' of individual shoppers (Anscombe 2017). Tellingly, these applications are beginning to shift from detection technology to identification technology as commercial outlets strive to link camera data with purchasing information. When facial recognition systems become widespread, detection applications (such as 'mood' inference) will also be implemented for purposes including marketing and

security. For instance, the US Department of Homeland Security is developing systems to infer ‘mal-intent’ (the intent to do harm) from visual and biometric cues (Ackerman 2017).

As these different examples illustrate, facial recognition is a demonstrably powerful and pervasive technology, and is prompting considerable enthusiasm and expectation. In a practical sense, facial recognition applications promise myriad benefits and conveniences including speedy and secure transactions, customised services, and enhanced public safety and security.

At its core, facial recognition transforms the process of identification from active targeting (as in the case of attempts to identify individual persons of interest) to passive and generalised recognition. By default, everyone who passes in front of a camera is identified. Moreover, these surveillance techniques draw upon the especially revelatory nature of geographical information – as Mayer (2013) argues, knowing where people go provides intimate and wide-ranging information about their professional, personal, and leisure lives. Keeping track of the when someone visits a marriage counsellor’s office, an abortion clinic, or an AA meeting can reveal highly sensitive personal information. While it is tempting to suggest that lifting the veil of anonymity heralds a return to pre-modern, pre-urban, village life, the rise of computer-driven facial recognition is qualitatively and quantitatively different. The ‘memories’ that are captured by automated systems are recorded and stored in digitised form, the monitoring is asymmetrical (people are seen, but the tracking systems often go un-noticed), and the image processing takes place at a massive scale. No human can recognise and identify all 50,000 faces in a football stadium in real-time, but digital camera systems are being developed to do so.

Problematising the rise of facial recognition

Certainly, computer-driven facial recognition is an emerging technology that will significantly transform our understandings and experiences of monitoring in a range of public and private spaces. On the one hand, it might be presumed that there is little to worry about. After all, many countries in the global north (not least the US, UK and Australia) have long been home to extensive networks of human-operated CCTV cameras. More esoterically, perhaps, the accepted premise of using facial morphological features as an indicator of mood, intention and personality stretches back to the Ancient Greek interest in physiognomy (Crawford and Paglen 2019). It is understandable, then, that many people are broadly welcoming (or at least begrudgingly accepting) of the various proclaimed benefits to deploying this technology: for example, more efficient and secure transactions, greater accountability, enhanced public safety and security, improved economic productivity, and commercial services.

Nevertheless, concerns are growing amongst some groups regarding the place of facial recognition technologies in democratic society. Imperatives being raised include issues of diminished accountability, compromised civil rights, and limitations on the concentration of power. As demonstrated in recent efforts to curtail the public use of facial recognition (such as the successful campaign to ban the use of facial recognition by San Francisco public agencies) these concerns are varied. First, is the potential for (and consequences of) misrecognition. For all its sophistication, computer-based facial recognition technology remains fallible. The past five years have seen repeated reports of facial recognition systems failing to recognise African American faces due to the racially skewed data-sets that the algorithms have been trained on (Noble 2018), alongside the ‘glitch’ of identical twins being able to confuse facial identification systems (King 2019). As such, there are concerns about large-scale misidentification (Brandom 2018) and machine bias in the form of systematic misrecognition by skin colour or ethnic background (Crawford and Paglen 2019). Recent studies suggest that we are still far short of having facial recognition systems that can accurately identify everyone in a large crowd (Reilly 2018), while some systems continue to work better on certain demographic groups than others (Simonite 2018).

Second, are concerns regarding the over-reach and ‘mission creep’ of these technologies – especially when used by authoritarian governments and/or commercial interests. For example,

the widespread use of facial recognition technology enables the creation of detailed databases about people's actions and whereabouts, raising a host of concerns about control over personal information and the uses to which it is put. In some Chinese cities, for example, facial recognition systems are used to identify and publicly shame jaywalkers by displaying their names on electronic billboards, and police are equipped with 'smart' glasses that identify criminal suspects (Dodds 2018). Facial recognition systems are also being used to target political dissidents and restrict their access to services including train and airplane travel (Carney 2018). Facial recognition systems can transform the spaces through which we move into a visual sensing system that promises to reconfigure our experience of what it means to be 'out in public' by making comprehensive tracking the rule rather than the exception. Moreover, smart cameras allow for new forms of 'function creep': as facial recognition technology develops it will likely treat the face not just as a form of biometric identification, but also as a new source of demographic and psychographic data. In short, this technology is set to significantly alter the ways in which people are known, as well as what constitutes available 'knowledge' for powerful social institutions. Employers, for example, are trialling automated job interview systems that measure facial 'microexpressions' to screen potential employees. Such systems create new forms of actionable 'knowledge' about individuals that can be used to sort and evaluate them. While it may be true that appearance and expression style have long played a role in hiring decisions, facial recognition automates and systematises this role.

Facial recognition technologies in education

Against this contentious background, then, we need to consider how these technologies are being applied to the specific context of education. While rarely foregrounded in debates about facial recognition in society, the school sector is one of the public settings where this technology is beginning to be taken up and implemented at scale. This is perhaps not surprising given, on the one hand, the role played by the classroom in the development of monitoring and disciplinary practices and, on the other, the increasing normalisation of surveillance in the name of protecting and securing young people.

One prominent educational application of facial recognition technology is campus security. This form of facial recognition is most prevalent in the US, where school shooting incidents have prompted school authorities to annually spend \$2.7 billion on-campus security products and services (Doffman 2018). Facial recognition systems have now been sold to thousands of US schools, with vendors 'pitching the technology as an all-seeing shield against school shootings' (Harwell 2018, n.p). As well as purporting to identify unauthorised intruders, systems have been developed to make use of video object classification trained to detect gun-shaped objects, alongside more subtle forms of 'anomaly detection' such as students arriving at school in different-than-usual clothes, bags and other apparel (Harwell 2018). These systems promise to give school authorities an ability to initially determine who is permitted onto a school campus, and then support the tracking of identified individuals around the school site. As the marketing for the SAFR school system reasons, the capacity to know where students and staff are means that 'schools can stay focused and better analyse potential threats' (SAFR 2019).

Another application of facial recognition in schools is attendance monitoring – promising to put an end to the inevitable gaps and omissions that arise when human teachers are tasked with repeatedly conducting roll-calls of large student groups (Puthea, Hartanto, and Hidayat 2017). This application of facial recognition is proving popular in countries such as the UK and Australia where school shootings and unauthorised campus incursions are rare. For example, the Australian 'Loop-Learn' facial recognition roll-call system has been marketed amidst estimates of saving up to 2.5 hours of teacher time per week. Elsewhere, automated registration systems are also considered an effective means of overcoming problems of 'fake attendance' and 'proxies' – especially in countries such as India where fraudulent attendance is commonplace (Wagh et al. 2015).

Beyond campus-based security and tracking physical bodies, facial recognition is also being used in a number of ‘virtual learning’ contexts. For example, facial recognition systems are now being developed as a means of ensuring the integrity of various aspects of online courses. This includes controlling access to online educational content (Montgomery and Marais 2014), as well as using webcam-based facial recognition to authenticate online learners (i.e., confirming that the people engaging in online learning activities are actually who they claim to be) (Valera, Valera, and Gelogo 2015). Similarly, there is a growing interest in using facial recognition technology for so-called e-assessment security – i.e., verifying the identity of students taking computer-based tests and examinations, and confirming their continued presence during the whole examination period (Hernández et al. 2008; Apampa, Wills, and Argles 2010).

Finally, there is a growing interest in facial detection techniques as an indicator of student ‘engagement’ and learning. For example, research and development in this area have reported that detecting brief ‘facial actions’ can prove an accurate indicator of students’ (non)engagement with online learning environments – highlighting episodes of boredom, confusion, delight, flow, frustration, and surprise (Dewan et al. 2019). Particularly insightful facial actions with regards to learning are reckoned to include brow-raising, eyelid tightening, and mouth dimpling (e.g., Graftsgaard et al. 2013). Elsewhere, it is claimed that ‘facial microexpression states’ (facial states lasting less than half a second) correlate strongly with conceptual learning, and ‘could perhaps give us a glimpse into what learners [a]re thinking’ (Liaw, Chiu, and Chou 2014). All told, there is growing interest in the face as a ‘continuous and non-intrusive way of... understand[ing] certain facets of the learner’s current state of mind’ (Dewan et al. 2019). Indeed, much of this work originates in the area of ‘emotion learning analytics’ that has long sought to use facial detection to elicit signs of learning in higher education. Here, learning scientists have focused on the use of facial detection of ‘academic emotions’ that convey achievement (contentment, anxiety, and frustration), engagement with the learning content, social emotions, and ‘epistemic’ emotions arising from cognitive processing. It is argued that detecting these emotions from facial expressions can highlight problems with knowledge, stimulation, anxiety and/or frustration (see D’Mello 2017).

These largely experimental developments have led some educationalists to enthusiastically anticipate facial learning detection being deployed on a mass scale. As Timms (2016, 712) reasons, it might soon be possible to gain a ‘real-time’ sense of which groups of students are in a ‘productive state’ and other instances ‘where the overall activity is not productive’. The promise of customisation that characterises the development of automated learning systems encourages their incorporation into student learning interfaces, so that these can recognise and respond to individual students in real-time, monitoring their achievements as well as their affective states. As these systems augment and eventually displace teacher-centred forms of instruction, they will need to be able to ‘recognise’ and respond to individual students. Automated systems underwrite the promise of customisation that has long characterised the online economy, offering to reconfigure it in the form of individualised tutoring, but without the expense of human teachers.

Making sense of the take-up of facial recognition technology in schools

As the 2020s continue, we are likely to see the steady adoption of these technologies (and those that will soon be following) in schools. Indeed, a small but growing number of US school districts are beginning to implement facial recognition security systems (Durkin 2019). At the same time, attempts are being made to integrate webcam-based facial recognition into commonly used learning platforms such as Moodle that are used by millions of students around the world (Guillén-Gómez, García-Magariño, and Prieto-Preboste 2014). At the same time, there seems to be little sustained opposition to the implementation of these technologies in schools – in contrast to more contentious discussions about the application of facial recognition in other areas of society. A recent survey of Australian public opinion found high levels of approval for the deployment of facial recognition systems in schools for purposes of ‘monitoring attendance and ensuring student safety’ (Selwyn 2019).

Indeed, this survey found the prospect of facial recognition in schools to attract notably higher levels of support from respondents than the prospect of online classes, automated essay grading and other already well-established forms of educational technology.

Schools are thereby positioned as relatively conducive contexts for the introduction of facial recognition technologies. This apparent ‘good fit’ between schools and facial recognition is supported by a couple of straightforward practicalities. First, is the infrastructural ease with which facial recognition can be implemented and adopted across schools. This is the technology that fits neatly with established school practices, processes and infrastructures. Crucially, schools have long traditions of routinely collecting and maintaining photographic records of students’ faces. Facial recognition systems are therefore able to appropriate existing name-and-face photographic databases. Moreover, as institutions with relatively stable populations, practical implementation of the technology is easier than in more ‘open’ institutional settings such as hospitals or libraries.

Another factor which may well be hastening the implementation of facial recognition systems in schools is their already extensive video monitoring and closed-circuit surveillance infrastructures. The past 20 years have seen the enthusiastic adoption of CCTV in the US, UK and Australian schools, meaning that many campuses already have surveillance camera systems with campus-wide coverage. In some instances, school enthusiasm for surveillance technologies has already seen the tentative adoption of teacher body-cameras, fingerprint enrolment and RFID-tagging of students. In the United States, the tragic litany of school shootings combined with the political failure to respond with firearm restrictions has resulted in the rise of surveillance-based ‘solutions’, including ‘smart cameras’ deployed as early warning systems. A company called ZeroEyes, for example, claims to have developed a smart camera system that can recognise an armed attacker and send an automated alert to local officials that includes an image with precise details about the location and weaponry of the suspect. The image recognition software pioneered by the company promises to transform the existing network of surveillance cameras from a deterrent system into a network of early responders (ZeroEyes 2019). A similar start-up called Athena, backed by Silicon Valley entrepreneur Peter Thiel, co-founder of PayPal and the security analytics company Palantir, claims that it has developed smart camera systems that can recognise patterns of behaviour that indicate violence or potential threat (Tucker 2019). Simultaneously, there has been a sustained push in some countries for video-based monitoring of classroom teachers in order to improve instructional practices (Strauss 2013). All told, facial recognition systems fit neatly into well-established school surveillance and monitoring cultures for both security and pedagogical purposes (Taylor 2012, Torres and Monahan 2009).

Nevertheless, despite these correspondences, there are a number of ways in which the emerging presence of facial recognition technology in schools might be questioned, if not robustly challenged. To date, any push-back against facial recognition in schools has tended to focus on discomforts around vaguely expressed notions of ‘privacy’ and/or doubts over the technical efficiency of particular systems. For example, the capacity of facial recognition systems to prevent hostile shooters has been criticised as little more than ‘security theatre’, with the technology argued to ‘offer only the appearance of safer schools’ (Andrew Ferguson – cited in Harwell 2018). Elsewhere, the Swedish ‘Datainspektionen’ recently began fining schools for adopting facial recognition roll-call systems – partly on the ground that ‘students’ consent could not be freely given because the school administration has a moral authority over them’ (Kayali 2019, n.p.). Yet, other than these occasional disjunctures, facial recognition technologies have so far faced a relatively unhindered passage into schools.

In terms of academic commentary, questioning to date of facial recognition in education has tended to focus on the pedagogical implications of using facial recognition and other biometric technologies as classroom tools to support learning and teaching assessment. For example, Kenneth Saltman (2016) argues that the logics of gauging emotions in order to influence subsequent decision-making is root in consumer marketing and the development of personalised advertising. He argues that the extension of this logic into classrooms (in the guise of personalised learning) infers a number of significant limiting assumptions and logics about learning and teaching. These include the

reduction of learning to a passive process of knowledge consumption, and teaching as a disciplined behaviour of ‘capturing student attention rather than engaging in dialogic exchange or dispositions for questioning, investigation, and experimentation’ (Saltman 2016, 57). In short this is a model of learning that marginalises issues of social context and ‘the inevitable cultural politics of knowledge’. These points are supported by Ben Williamson (2017) who highlights these classroom applications of facial recognition as part of a wider push to use biometrics as a form of ‘persuasive computing’ that reframes teaching and learning in terms of individualised ‘psychological behaviour change techniques’ (128). In this sense, learning is reduced to a set of psychological traits and characteristics that are discernible through the face, and are open to manipulation (see also Williamson and Piattoeva 2019).

Challenging the take-up of facial recognition in schools

These questions over diminished notions of pedagogy and consent are important. Yet, at this point, we would like to argue that there are a number of additional issues and concerns that cast further serious doubt upon the implementation of facial recognition technologies in schools. In brief, the following points of contention might be raised:

(i) The dehumanising nature of facially focused schooling

First is the argument that the statistical processes through which facial recognition technologies quantify and frame a student’s face are inherently reductive. As noted earlier, facial recognition technologies work by assigning numerical values to schematic representations of facial features, and then making comparisons between those values. Antoine Bousquet (2018) characterises this as a ‘linear perspective’ based on the geometric/ mathematical conceptualisation of space. The mechanistic gaze of facial recognition, therefore, consists solely of the extraction and abstraction of a student’s most personal features from what are essentially statistical images. As Bousquet (2019) continues, the majority of these images never pass in front of human eyes, but are subject to intensive algorithmic treatment and synchronised with similarly decontextualised statistical geospatial information.

This constitutes a very reductive engagement with students in contrast to how they would ordinarily be viewed by a human. Students are not ‘seen’ by facial recognition technologies in a manner that is able to discern their full range of facial emotions – for example, someone who is utterly bereft or someone who has a glimmer of recognition. Indeed, one of the likely practical consequences of facial recognition technologies is students having to contort their facial expressions in ‘unnatural’ ways that allow the technology to ‘detect’ and/or ‘recognise’ them. If the cold algorithmic gaze of the system is not triggered, then the onus is on the student to present a different (more ‘readable’) face. More cynical students looking to ‘game the system’ might perfect their ability to dimple their mouth and thereby be classified as ‘learning’. While these adjustments might seem like minor inconveniences, it could be argued that this lack of full acknowledgement for what are amongst any individual’s most personal attributes is inevitably dehumanising and distancing.

(ii) The foregrounding of students’ gender and race

Another unsettling reduction of facial recognition technologies is their role in foregrounding fixed attributions of students’ race and gender in informing school decision-making. As noted earlier, frequent concern has been raised over the disproportionate emphasis that facial recognition places on ‘detecting’ the gender and race of those individuals that it identifies. As Luke Stark (2019) observes, the ways in which these technologies schematise human faces foregrounds ‘calculations’ of race and gender as a means of arbitrarily dividing human populations. As mentioned earlier, this has been highlighted in recent high-profile controversies over the inability of some facial detection systems

to ‘successfully’ discern non-white faces due to the racially skewed databases that these systems have been trained on.

Yet, even if these identifications are rendered more technically accurate, it can be argued that sorting students into socially constructed racialised and/or gendered categories remains a discriminatory practice – conflating biological characteristics with social attributes. The development of facial recognition technology has helped resuscitate long-debunked race ‘science’ by attempting to formalise phenotypic differences – an endeavour that tends, seemingly irresistibly, to spill over into claims about genetic capabilities and aptitudes. Facial recognition technologies will certainly foreground issues of race within schools, and therefore exacerbate any pre-existing racially discriminatory practices. As Stark (2019, 53) reasons: ‘If human societies were not racist, facial recognition technologies would incline them toward racism; as human societies are often racist, facial recognition exacerbates that animus’. This argument holds true for schools as much as any other societal institution.

(iii) The inescapable nature of school-based facial recognition

Another point of concern is the inescapability of facial monitoring within school contexts. Unlike other forms of personal data (i.e., any piece of data connected to an individual’s name), facial data lends itself to constant and permanent surveillance. In short, people are always connected to their faces. Thus, unlike social media posts or interactions with school learning management systems, there is no option for students to self-curate and restrict what data they ‘share’. While students might be able to opt-out from facial detection elements of their school’s learning systems (for example, the use of eye-tracking or facial thermal imaging for learning analytics), there is no right to decline to participate in ‘non-cooperative’ facial recognition systems (indeed, any opt-out effectively renders campus facial recognition systems ineffective).

While such coercion applies to the use of facial recognition in all public spaces, it is especially acute in schools. For example, most schools enforce dress codes that preclude students’ faces being covered by hair, hoods or other obtrusions. This makes it difficult for students to obscure their faces from surveillance cameras. This also raises the inadequacy of any promise of ‘informed consent’ regarding school facial recognition systems. The systems being deployed in schools for security and attendance purposes rely on complete sweeps of classrooms and corridors in order to operate. This renders ‘opt-in’ and ‘out-out’ approaches counter-productive from the point of view of the system provider. Even if opt-out protocols are in place, the system has to scan a student’s face before it can recognise that they have opted out.

(iv) The elimination of obscurity

Proponents of facial recognition (and surveillance technology in general) usually counter criticism of compulsory scanning with arguments along the lines of ‘if you have nothing to hide then you have nothing to fear’. While questionable in any context, this argument overlooks the value for some students to have an opportunity to hide while in school. Indeed, the constant surveillance of campus facial recognition equates with a substantial curtailment in students’ right to obscurity while in school. In short, students will find it increasingly difficult to blend into the background, take a back seat, and generally go about their business ‘under the radar’.

These might seem like undesirable behaviours from an educational point of view, yet for specific groups of students, these are legitimate coping strategies and an invaluable means of ‘doing’ school on their own terms. Schools can be fraught places for children and young people to develop a sense of social identity and confidence, and much emphasis is now placed on making schools socially supportive and nurturing settings. In this sense, attempting to manage what is known and disclosed about oneself can be seen as a legitimate way of students ensuring that their actions and intentions

are correctly interpreted and understood (Gordon, Holland, and Lahelma 2000). In contrast, facial recognition systems lead to what Hartzog and Selinger (2018, n.p) term ‘the normalized elimination of practical obscurity’.

(v) The increased authoritarian nature of schooling

Following on from this point, Hartzog and Selinger (2018, n.p) make the blunt point that ‘surveillance conducted with facial recognition systems is intrinsically oppressive’. As acknowledged earlier, facial recognition technologies are most likely to be implemented with the intention of controlling who enters a school, and where they subsequently are located. Of course, schools are institutions whose function is to regulate, control, and discipline the minds and bodies of students. In this sense, facial recognition technologies fit well with the historical purposes and structures of schools. As such, these technologies are most likely to exacerbate (and certainly not mitigate) the authoritarian tendencies of the schools within which they are implemented. As Hartzog and Selinger (2018, n.p) argue, ‘the sheer intoxicant of power will tempt overreach, motivate mission creep, and ultimately lead to systematic abuse’. There is also a good chance that facial recognition technologies will prompt students to act differently and normalise their conduct. As Hartzog and Selinger (2018, n.p) put it, facial recognition invariably results in ‘impeding crucial opportunities for human flourishing’. In contrast, supporting the flourishing of students is an integral purpose and goal of schooling.

(vi) The cascading logic of automation

Facial recognition systems rely on automated, passive, data capture to create a new biometric, geo-tagged database. One of the lessons we have learned in recent years, is that automated information collection leads to what might be described as a cascading process of automation: large databases require automated information processing, which, in turn, leads to automated decision-making processes. The installation of smart camera networks does not just introduce a new monitoring tool, it also results in the creation of new databases that can be used for a growing range of purposes, from automated risk detection (and response) to automated content customisation. This is a question of both function creep, and the displacement of human judgement by automated decision-making processes. Once facial recognition is implemented, for example, it can take on a variety of functions from attendance to lunch payment, to expression recognition (for the purposes of both security and pedagogy). The result is the subtraction of humans from the decision chain – an outcome that may address the needs of cash-strapped schools (although the technology can be expensive), but which runs the risk of what might be called ‘social de-skilling’ when it comes to recognising student needs and coming to terms with their behaviour. While there may be advantages in terms of speed, efficiency, and customisation based on automated data-collection systems, there is also the danger of undermining important forms of socialisation that are part of the learning process.

(vii) The future oppression of marginalised groups within schools

Finally, facial recognition techniques embody an ambition to control and standardise the actions and behaviours of students’ lives – arguably one of the central premises upon which contemporary digital society is founded. From this perspective, the students who stand to be harmed most by facial recognition technologies in schools are those who do *not* fit neatly into standardised systems, and those whose lives fall between the cracks of dataveillance. In short, the concern remains that the ways in which data derived from facial recognition systems will be used in conjunction with other aspects of the datafied school does not advantage outliers or those whose lives do not fit neatly into discrete categories.

Referring back to our earlier observations over the foregrounding of race by facial recognition technology, it seems likely that this technology will be implicated in reproducing racialised class hierarchies within school contexts that have longstanding social and cultural reproduction processes (see Lewis and Diamond 2015). Another such obvious group is queer and trans students in what continue to be profoundly heteronormative school contexts. This is illustrated in Os Keyes (2019, n.p) provocative argument that, ‘data science is a profound threat for queer people’. Defining ‘queer’ primarily in terms of fluidity, autonomy, a distinct lack of definition and ‘the freedom to set one’s own path’, Keyes reasons that data-driven technologies such as facial recognition are fundamentally set in opposition to these qualities (grounded as data science is in norms, discrete categories, precise definitions and assumptions of predictable futures). Any gaps, omissions and blanks in non-binary and non-conforming students’ data profiles will invariably lead to diminished calculations and a limited range of diagnoses and decisions being made about them. Significant issues are likely to be ignored, or perhaps additional unwarranted assumptions made. Either way, the chances of these students being misrepresented are high.

Discussion

Whether or not facial recognition ‘works’ as promised by its developers and vendors, this technology looks set to be integrated increasingly into school settings by actors who are motivated to think and act otherwise. As Adam Greenfield (2018, 243) contends, ‘the meaningful question isn’t whether these technologies work as advertised. It’s whether someone *believes* that they do, and acts on that belief’. Against this background, then, there is a need to treat the continued integration of these technologies into schools as a serious (and potentially alarming) proposition. As is always the case with any ‘new’ technology, it is important to reflect upon what is *not* being talked about and/or what issues are no longer being talked about in the same ways. It is also important to consider the most undesirable consequences that might result. Regardless of any perceived institutional and/or educational benefits, these are technologies that need to be considered in problematic terms.

In this sense, it is important to reflect on the distinct social order that is being built up around facial recognition and schools – i.e., likely reconfigurations of power, (dis)advantage and relations within school settings. When approached in these terms, there is much about facial recognition in schools that merits further consideration. Yet in light of the issues and concerns raised in the latter half of this article, perhaps the most pressing concern for the time being is the basic question of whether or not any of these technologies have a justifiable place in schools.

To date, this has not been a point of contention amongst education professionals and/or education publics. Indeed, most of the counterpoints rehearsed in this paper have yet to feature in public, political or professional debates about the increased implementation of facial technologies in schools. Yet, clearly these are technologies that raise a number of concerns when implemented in school settings. Indeed, some of the arguments detailed toward the end of this paper suggest the outright banning of facial recognition technologies in schools. Hartzog and Sellinger (2018, n.p) conclude that facial recognition constitutes ‘the most uniquely dangerous surveillance mechanism ever invented’. Stark (2019) concurs with these arguments, arguing for the shutdown of these technologies in all but the most controlled circumstances. As Kate Crawford (2019, 565) concludes, ‘these tools are dangerous when they fail and harmful when they work’.

Of course, the standard response from a technical point of view is that system developers and school communities need to work harder to ensure that there are no such gaps and omissions. For example, in terms of concerns over the reductive nature of what can be known through facial recognition and/or current propensities for mis-recognition of minority groups, the generally accepted response is for developers to continue working to expand the reach and scope of facial-recognition surveillance. Suggestions along these lines tend to include training systems on more diverse training data-sets, ensuring that more finely grained data are collected about the broader

characteristics of ‘who’ each student is, and generally working to increase students’ data visibility and participation in the continual production and analysis of facial recognition data.

Such adjustments might improve the technical calibration of facial recognition systems in schools, yet would do little address the more fundamental concerns of othering, oppression and coercive control. In terms of these latter issues, it makes little sense for students (and teachers) to actively work to legitimise inhumane forms of datafied schooling. As Os Keyes (2019, n.p.) puts it, ‘I don’t know about you, but my idea of a solution to being othered by ubiquitous tracking is not “track me better”’. As such, Keyes contends that there is little point fighting to reform and improve data-driven systems whose operation harms marginalised populations. For example, training facial recognition systems on more diverse data sets so that they recognise black faces more ‘accurately’ simply increases the harm that these systems can then do to black students. It could be argued that a more logical response would be for students and staff to refuse to participate in such systems that are fundamentally designed to arbitrarily divide, control and do harm to whole school communities.

Yet, while a strong case might be made for total rejection of facial recognition technology across society, this translates awkwardly for students who are entrenched in school contexts that are by their very nature coercive, controlling and disciplinary. Most students are not in a practical position to directly refuse their school’s surveillance infrastructure (any more than they can completely opt-out of their school’s dress code, timetabling and various other impositions and regulations). Thus, the most likely *realistic* responses to the imposition of facial recognition technology in schools are likely to be bottom-up, emergent, sporadic and playful – in de Certeau’s (1984) terms, these are technological structures that are best countered through the deployment of improvised and opportunistic ‘tactics’. In this sense, we now need to properly explore (both through further refinement of the arguments rehearsed in this paper and also empirical inquiry), how students, teachers and others located within schools might work realistically toward non-participation, resistance and (perhaps) reinvention of facial recognition technologies.

For example, this might include thinking how educators and educationalists might engage in sustained collective sense-making and critique with regards to facial recognition in schools. It should also include exploring what practical opportunities there might be for students to engage in facial data obfuscation and other forms of algorithmic counteraction – for example, what Zach Blas (2013) describes as tactics of ‘facelessness’ and ‘defacements’ (such as wearing masks, asymmetrical hairstyles and face adornments). At the same time, this might involve giving proper consideration to possible opportunities for students and teachers to surreptitiously repurpose and/or reshape their schools’ uses of facial recognition through their everyday actions. Indeed, as facial recognition technology becomes cheaper and integrated into consumer electronics (i.e., on smartphones), we need to give proper consideration to how students might begin to utilise their own facial recognition technologies – perhaps in *sousveillance* ways, or ways that generate alternate information streams and/or ways of knowing.

Conclusion

Facial recognition is a far-reaching technology that the education sector needs to pay sustained attention to throughout the 2020s. Regardless of any concerns raised in this article, these technologies will continue to be taken up by schools with various intentions and justifications – from boosting school safety in the wake of campus shootings, through to better directing teacher attention within a classroom. Yet, despite the fact that we are on the cusp of its widespread implementation, the implications of facial recognition use in schools have yet to be considered systematically. In this article, we have attempted to initiate a conversation about the implications of allowing these technologies into schools. These are discussion points that we look forward to being tested, challenged and refined by educational commentators over the next few years.

Above all, then, is the need to thoroughly discuss the basic question of whether these technologies have a place at all within school contexts. Indeed, a strong case can be made that any ‘added value’ or

gained ‘efficiencies’ are outweighed by the consequences of automated sorting and classification for students. What might appear to be the relatively benign implementation of a new digital technology in school is perhaps a case of what Stark (2019, 54) terms ‘trading off its enormous risks for relatively meagre gains’. This raises the concern that schools are being co-opted as sites for the normalisation of what is a ‘societally dangerous’ technology – what Stark (2019, 55) describes as a ‘facial privacy loss leader’. Thus, it can be strongly argued that schools should not be places where local communities become desensitised to being automatically identified, profiled, and potentially discriminated against. The key challenge now facing educators is whether or not there is a realistic future prospect of somehow reshaping these technologies for more beneficial and/or benign purposes. Alternatively, is this a form of digital technology that should not be ‘educationally’ applied in any form whatsoever?

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Mark Andrejevic is Professor of Media and Communication at Monash University, Australia. He writes about surveillance, popular culture and digital media and is the author of, *Reality TV: The Work of Being Watched*, *iSpy: Surveillance and Power in the Interactive Era*, and *Infoglut: How Too Much Information is Changing the Way We Think and Know*. He is a member of the NSF-funded Council for Big Data, Ethics, and Society and heads the Culture, Media, and Economy Focus Program at Monash University.

Neil Selwyn is a Distinguished Research Professor at the Faculty of Education, Monash University, Australia. His research and teaching focus on the place of digital media in everyday life, and the sociology of technology (non)use in educational settings. Neil is the author of, *Distrusting Educational Technology, Is Technology Good For Education?*, and *What Is Digital Sociology?*

ORCID

Neil Selwyn  <http://orcid.org/0000-0001-9489-2692>

References

- Ackerman, S. 2017. “TSA Screening Program Risks Racial Profiling Amid Shaky Science – Study Says.” *The Guardian*, February 8. <https://www.theguardian.com/us-news/2017/feb/08/tsa-screening-racial-religious-profiling-aclu-study>.
- Anscombe, L. 2017. “Westfield is Using Facial Detection Software to Watch How You Shop.” *News.Com.au*, October 19. <https://www.news.com.au/finance/business/retail/westfield-is-using-facial-detection-software-to-watch-how-you-shop/news-story/7d0653eb21fe1b07be51d508bfe46262>.
- Apampa, K., G. Wills, and D. Argles. 2010. “An Approach to Presence Verification in Summative e-Assessment Security.” In 2010 International Conference on Information Society, 647–651. IEEE.
- Blas, Z. 2013. “Escaping the face.in *Media-N*.” CAA Conference Edition, Summer, 9(2).
- Bolger, R. 2018. “Cafe App that Knows How You Take Your Coffee Sparks Security Concerns.” *SBS News*, January 5. <https://www.sbs.com.au/news/cafe-app-that-knows-how-you-take-your-coffee-sparks-security-concerns>.
- Bousquet, A. 2018. *The Eye of War: Military Perception from the Telescope to the Drone*. Minneapolis: University of Minnesota Press.
- Brandom, R. 2018. “Amazon’s Facial Recognition Matched 28 Members of Congress to Criminal Mugshots.” *The Verge*, July 26. www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.
- Burt, C. 2018. “Australia Considers Deploying Unisys Facial Recognition Technology for Social Media Checks at Airports.” *Biometric Update*, www.biometricupdate.com/201809/australia-considers-deploying-unisys-facial-recognition-technology-for-social-media-checks-at-airports.
- Carney, M. 2018. “Leave No Dark Corner. *ABC News*, September 18.” <http://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278>.
- Crawford, K. 2019. “Regulate Facial-Recognition Technology.” *Nature* 572 (29th August): 565.
- Crawford, K., and T. Paglen. 2019. *Excavating AI: The politics of Images in Machine Learning Training Sets*. www.excavating.ai.

- de Certeau, M. 1984. *The Practice of Everyday Life*. Translated by Steven Rendall. Berkeley: University of California Press.
- Dewan, M., A. Akber, M. Murshed, and F. Lin. 2019. "Engagement Detection in Online Learning: A Review." *Smart Learning Environments* 6 (1): 1.
- D'Mello, S. 2017. "Emotional Learning Analytics." In *Handbook of Learning Analytics*, edited by C. Lang, G. Siemens, A. Wise, and D. Gašević, 115–127. Sydney: SoLAR.
- Dodds, L. 2018. "Chinese Businesswoman Accused of Jaywalking After AI Camera Spots Her Face on an Advert." *The Daily Telegraph*, November 25.
- Doffman, Z. (2018). Why facial recognition in schools seems to be an aimless recipe for disaster. Forbes, 7th November, www.forbes.com/sites/zakdoffman/2018/11/07/why-facial-recognition-in-schools-seems-to-be-an-aimless-recipefordisaster/#7abc4f01a83a
- Durkin, E. 2019. "New York School District's Facial Recognition System Sparks Privacy Fears." *The Guardian*, May 31.
- Gordon, T., J. Holland, and E. Lahelma. 2000. "Who are the Wallflowers?" In *Making Spaces: Citizenship and Difference in Schools*, edited by J. Campling, 192–203. London: Palgrave Macmillan.
- Grafsgaard, J., J. Wiggins, K. Boyer, E. Wiebe, and J. Lester. 2013. Automatically Recognizing Facial Expression: Predicting Engagement and Frustration." International Conference on Educational Data Mining, Memphis.
- Greenfield, A. 2018. *Radical Technologies*. London: Verso.
- Grubb, B. 2018. "Facial Recognition's Ominous Rise: Are We Going Too Far Too Fast?" *Sydney Morning Herald*, January 3. <https://www.smh.com.au/technology/facial-recognition-s-ominous-rise-are-we-going-too-far-too-fast-20180103-p4yy7d.html>.
- Guillén-Gámez, F., I. García-Magariño, and S. Prieto-Preboste. 2014. "Facial Authentication Within Moodle Lessons." *Contemporary Engineering Sciences* 7 (8): 391–395.
- Hartzog and Selinger. 2018. "Facial Recognition is the Perfect Tool for Oppression." *Medium*, August 3, <https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66>.
- Harwell, D. 2018. "Unproven Facial-Recognition Companies Target Schools, Promising an End to Shootings." *Washington Post*, June 7.
- Hernández, J., A. Ortiz, J. Andaverde, and G. Burlak. 2008. "Biometrics in Online Assessments: A Study Case in High School Students." In 18th International Conference on Electronics, Communications and Computers (conielcomp 2008), 111–116. IEEE.
- Kayali, L. 2019. "How Facial Recognition is Taking Over a French City." *Politico*, September 26. www.politico.eu/article/how-facial-recognition-is-taking-over-a-french-riviera-city/.
- Keyes, O. 2019. "Counting the Countless." *Real Life*, April 8.
- Khalfallah, J., and J. Slama. 2015. "Facial Expression Recognition for Intelligent Tutoring Systems in Remote Laboratories Platform." *Procedia Computer Science* 73: 274–281.
- King, E. 2019. "Twin Faces and Algorithmic Image Cultures." Paper presented at the Resisting Digital Culture Conference, London, May 10.
- Lewis, A., and J. Diamond. 2015. *Despite the Best Intentions: How Racial Inequality Thrives in Good Schools*. Oxford: Oxford University Press.
- Liaw, H., M. Chiu, and C. Chou. 2014. "Using Facial Recognition Technology in the Exploration of Student Responses to Conceptual Conflict Phenomenon." *Chemistry Education Research and Practice* 15 (4): 824–834.
- Mayer, J. 2013. "What's the Matter with Metadata?" *The New Yorker*, June 6. <https://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata>.
- Monahan, T., and R. Torres. 2009. *Schools Under Surveillance*. New Brunswick, NJ: Rutgers University Press.
- Montgomery, J., and A. Marais. 2014. Educational Content Access Control System. U.S. Patent Application 14/212,069, filed September 18, 2014.
- Noble, S. 2018. *Algorithms of Oppression*. New York: New York University Press.
- Otwell, K. 2014. Facial Expression Recognition in Educational Learning Systems. U.S. Patent Application 14/086,695, filed June 5, 2014.
- Puthea, K., R. Hartanto, and R. Hidayat. 2017. "A Review Paper on Attendance Marking System Based on Face Recognition." In 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 304–309. IEEE.
- Reilly, C. 2018. "Facial-Recognition Software Inaccurate in 98% of Cases, Report Finds." *Cnet.com*, May 13. <https://www.cnet.com/news/facial-recognition-software-inaccurate-in-98-of-metropolitan-police-cases-reports/>.
- SAFR. 2019. *Introducing SAFR Facial Recognition for K-12 Schools*. <https://safr.com/k12/>.
- Saltman, K. 2016. *Scripted Bodies*. London: Routledge.
- Selwyn, N. 2019. *Digital Lessons? Public Opinions on the Use of Digital Technologies in Australian Schools*. Melbourne, Monash University – https://www.monash.edu/__data/assets/pdf_file/0008/1626236/Education-Futures-Research-Report-Digital-Lessons.pdf.
- Simonite, T. 2018. "How Coders are Fighting Bias in Facial Recognition Technology." *Wired*, March 29. <https://www.wired.com/story/how-coders-are-fighting-bias-in-facial-recognition-software>.
- Stark, L. 2019. Facial Recognition is the Plutonium of AI. *XRDS – Crosswords (ACM)*, April 2019.

- Strauss, V. 2013. "Bill Gates's \$5 Billion Plan to Videotape America's Teachers." *Washington Post*, May 10.
- Taylor, E. 2012. "The Rise of the Surveillance School." In *Routledge Handbook of Surveillance Studies*, edited by Kirstie Ball, Kevin Haggerty, and David Lyon, 225–231. London: Routledge.
- Timms, M. 2016. "Letting Artificial Intelligence in Education Out of the box." *International Journal of Artificial Intelligence in Education* 26 (2): 701–712.
- Valera, J., J. Valera, and Y. Gelogo. 2015. "A Review on Facial Recognition for Online Learning Authentication." In 8th International Conference on Bio-Science and Bio-Technology (BSBT), 16–19. IEEE.
- Vatrapu, R., P. Reimann, S. Bull, and M. Johnson. 2013. "An Eye-Tracking Study of Notational, Informational, and Emotional Aspects of Learning Analytics Representations." In *Proceedings of the Third International Conference on Learning Analytics and Knowledge*, 125–134. ACM.
- Wagh, P., R. Thakare, J. Chaudhari, and S. Patil. 2015. "Attendance System Based on Face Recognition Using Eigen Face and PCA Algorithms." In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 303–308. IEEE.
- Williamson, B. 2017. *Big Data in Education*. London: Sage.
- Williamson, B., and N. Piattoeva. 2019. "Objectivity as Standardization in Data-Scientific Education Policy, Technology and Governance." *Learning, Media and Technology* 44 (1): 64–76.
- Zero-Eyes. 2019. *School security*. <https://zeroeyes.com/school-security>.