Surveillance and Education

DAVID ROSEN AND AARON SANTESSO*

Few contemporary spaces are as thoroughly surveilled as the classroom. And yet, because educational surveillance consists not of one dominant activity, but of several semi-autonomous practices, which are not often thought of as related, it has attracted far less attention than, say, the bulk gathering of metadata by government security agencies. This paper undertakes to begin tracing the connections between, among other things, the in-classroom use of CCTV cameras; the spread of assessment and testing-regimes; dataveillance by providers of educational products; and the replacement of face-to-face learning by Massive Open Online Courses (MOOCs). To date, legal recourse against these initiatives has been a piecemeal affair, centreing around issues like the parental control of information about children, or job security for teachers.

This paper argues that the various and scattered modes of educational surveillance can be understood as connected through one issue: privacy rights. In the American tradition (going back to Warren and Brandeis, 1890), privacy is understood as a necessary precondition for the formation of an autonomous person. This paper argues that, in its various forms, educational surveillance has the effect of interrupting or manipulating this maturation process. Although the motives for this manipulation (by governments or businesses) differ, its effects can be explored in the traits ascribed to the so-called millennial generation (those born between 1982 and 2004). The paper concludes by relating the effects of educational surveillance to the larger separation of the very rich from everyone else, a process occurring on multiple vectors in society today.

* DAVID ROSEN: Professor of English, Trinity College, Hartford (email: david.rosen@trincoll.edu). AARON SANTESSO: Associate Professor of Literature at the Georgia Institute of Technology (email: aaron.santesso@lmc.gatech.edu).

In April 2014, a non-profit corporation known as inBloom quietly ceased operations. Although it had been founded as recently as 2011, with more than $100 million in seed money from the Bill and Melinda Gates Foundation, as well as the Carnegie Corporation of New York, inBloom had quickly found itself at the centre of several acrimonious debates about the new education economy, and specifically about the legality of new monitoring technologies in the classroom.[1] According to the company's own publicity materials, inBloom operated

> … a set of shared technology services, [including] middleware for identity management and data integration [designed to] provide educators, parents, elementary and secondary school students with learning data from many sources and connect them to relevant instructional resources to support personalized learning …[2]

In plain English, the ultimate goal of inBloom was to collect and aggregate information on every pre-college student in the United States, and then tie that information to the dispersal of 'relevant instructional resources'—i.e. pedagogical products. Although inBloom was itself a non-profit, the vendors with whom it shared its data were not: the Software Information Industry Association estimates the American market for primary and secondary-level educational software to be roughly $8 billion per annum.[3]

Few contemporary spaces are as thoroughly surveilled as the classroom. And yet, because educational surveillance consists not of one dominant activity, but of several semi-autonomous practices, which are not often thought of as related, it has attracted far less attention than (to pick some obvious examples) surveillance by government bodies like the NSA or certain kinds of corporate data-

[1] Valerie Strauss, '$100 Million Gates-Funded Student Data Project Ends in Failure' *Washington Post* (Washington, 21 April 2014).

[2] inBloom, 'Privacy and Security Policy' (*inBloom*, 2 January 2014) <www.inbloom.org/privacy-security-policy.html> [site since taken down, archive version of the page available at <http://web.archive.org/web/20140809060725/https://www.inbloom.org/privacy-security-policy.html> accessed 21 November 2014].

[3] Natasha Singer, 'Deciding Who Sees Students' Data' *New York Times* (New York, 5 October 2013).

mining. Among the principal modes of educational surveillance, we would note the following: first, and most prominently, the aggressive monitoring of both students and teachers, both inside and outside the classroom. While many of the more than 400 data fields inBloom provided for each student tracked test scores and other purportedly objective metrics, others were more intimate or subjective, such as 'disability, family [relationship], and disciplinary data.'[4] Many of the latter fields were optional – but the pressures towards completeness, to present a full picture of the child, were considerable. This tracking, taken to its logical conclusion, would follow its targets fully into their private lives. A US Department of Education position paper from 2012 suggests that 'data analytics' might detect 'boredom from patterns of [a student's] key clicks'; if these analytics were applied to work done at home, there would be 'a real possibility of continuous improvement via multiple feedback loops that operate at different time scales—immediate to the student, [and] daily to the teacher for the next day's teaching.'[5] Second, and related, we would note the increasing presence of cameras in the classroom – again, trained on both students and teachers. CCTV is already widely in use in US schools, usually in the name of security, but several advocates for 'educational reform' have called for more expansive applications. As Bill Gates commented in a May 2013 TED talk,

> I know some teachers aren't immediately comfortable with the idea of a camera in the classroom. [But] our experience … suggests that if teachers … collect video, … a lot of them will be eager to participate. Building this system also requires a considerable investment … up to five billion dollars. Now that's a big number, but to put it

[4] Letter from Secretary of Education Arne Duncan to Senator Edward Markey (22 October 2013) <www.markey.senate.gov/imo/media/doc/2013-10-22_FERPA.pdf> accessed 21 November 2014.

[5] Marie Bienkowski, Mingyu Feng, and Barbara Means, 'Enhancing Teaching and Learning through Educational Data Mining and Learning Analytics: An Issue Brief' (*US Department of Education*, October 2012). Note: This report was prepared for the Department of Education, not necessarily endorsed by it.

> in perspective, it's less than two percent of what we spend every year on teacher salaries.[6]

Gates's last observation, about the economics of contemporary education, gestures towards a whole larger class of practices, which, if not 'forms' of surveillance, strictly speaking, are nevertheless heavily dependent on surveillance or surveillance-friendly. Massive Open Online Courses, or MOOCs, for example, have begun to gain traction in some sectors of academia precisely as a way to save on 'teacher salaries', with in-classroom experiences replaced by computer-work.[7] Learning acquired online, as it happens, is also particularly conducive both to measurement and surveillance—surveillance in essence providing the 'justification' for this kind of learning. In the words of a White House-commissioned report,

> Data from a student's experience in [MOOCs] or other technology-based learning platforms can be precisely tracked, opening the door to understanding how students move through a learning trajectory with greater fidelity, and at greater scale, than traditional education research is able to achieve.[8]

We will take the opportunity, later in this paper, to question some of the assumptions behind these statements. For now, we would simply observe that MOOCs provide just one instance of how surveillance is used to underwrite the vast program of quantified learning that goes under the umbrella term 'assessment'.

---

[6] Bill Gates, 'Teachers Need Real Feedback' (*TED Talks Education*, May 2013) <www.ted.com/talks/bill_gates_teachers_need_real_feedback/transcript> accessed 21 November 2014

[7] Letter from the President's Council of Advisors on Science and Technology (PCAST) to President Barack Obama (December 2013) 4 <www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_edit_dec-2013.pdf> accessed 21 November 2014. '[O]ne possible trajectory for the MOOC technology would be to reduce the cost of education simply by economizing on the use of teachers, using computerized feedback to support a course rather than online or offline personal guidance by a faculty member or teaching assistant.'

[8] Executive Office of the President, 'Big Data: Seizing Opportunities, Preserving Values' (*The White House*, May 2014) 24-25 <www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf> accessed 21 November 2014.

inBloom, to be clear, was but one player in the area of educational surveillance; indeed, its exit from the field has simply opened the door for other, similarly-directed companies.[9] Nevertheless, the sheer scale of inBloom's ambitions, the clarity with which it drew together the various strands of educational surveillance, and the explicitness with which it laid bare the profit motive underlying much purported 'reform', all doubtless played roles in drawing hostile attention from advocacy groups and lawmakers. Not surprisingly, most of this criticism turned on the question of privacy, which has been defined mainly as the control of personally identifiable information (PII). Once vast amounts of PII, much of it highly sensitive, have been collected about a child, who then controls that data, and for how long should that information be preserved? Once the data have been passed along to third-party vendors (ostensibly to better craft educational 'products'), who then ensures that these vendors, whose principle motives are economic, will use the information responsibly, and prevent it from spreading? The US has long had statutes in place protecting the personal information of students, most notably the Family Educational Rights and Privacy Act (FERPA) of 1974—but successive revisions by the Bush and Obama administrations (in 2008 and 2011, respectively) have significantly reduced parental control over student records.[10]

In an October 2013 letter to the Secretary of Education Arne Duncan, Senator Edward Markey gave public voice to these concerns. Referring not just to inBloom, but to 'data storage [by] private companies' in general, Markey wrote: 'disclosure of [student data], which may extend well beyond the specific private company hired by [a] school district to a constellation of other firms with which the district does not have a business relationship, raises concerns about [student privacy].' Secretary Duncan's response, echoing inBloom's own stated privacy policy, was that 'as a practical matter, the Department [of Education] cannot monitor the many

[9] Olga Kharif, 'Privacy Fears Over Student Data Tracking Lead to InBloom's Shutdown' *Bloomberg Businessweek* (New York, 1 May 2014). Several competitors to inBloom are as active in the UK as in the US (Pearson, for example).

[10] Marc Rotenberg and Khaliah Barnes, 'Amassing Student Data and Dissipating Privacy Rights' (2013) 48(1) EDUCAUSE Review 56: the 2008 and 2011 amendments to FERPA 'increased private company and third-party access to student data'.

thousands of individual contracts between schools and third parties. Rather, we promote best practices and increased understanding of FERPA.'[11] In contrast to the UK, where the regulation of private student records is highly centralized, the US system leaves most decision-making power to individual school districts. Unfortunately, as a 2013 study undertaken by Fordham University's Center on Law and Information Policy revealed, '20% of districts fail to have policies governing the use of online services, and a sizeable plurality of districts have rampant gaps in their contract documentation, including missing privacy policies.' Moreover,

> fewer than 7% of agreements [between districts and third-party vendors] restrict the sale or marketing of student information by vendors, and many agreements allow vendors to change the terms without notice. [These] service agreements even allow vendors to retain information in perpetuity with alarming frequency.[12]

To repeat: in the debates that have swirled around inBloom and its ilk, privacy has been presented as having mainly to do with the control of PII. Tactically, this makes sense: the control of personal information is a cause most people can easily understand and rally around. With remarkable speed, in the fall of 2013 and spring of 2014, legal and public agitation made it impossible for inBloom to continue operations.[13] Without minimising the importance of information control, however, we would suggest that something even more fundamental is at stake when privacy is lost due to educational surveillance. To understand why, we must step back. Privacy law in America has its own peculiar history. Nearly all

[11] Letter: Duncan/Markey (n 4) 8.

[12] Joel Reidenberg and others, 'Privacy and Cloud Computing in Public Schools' (*Center on Law and Information Policy at Fordham Law School*, 12 December 2013) 6 <http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip> accessed 21 November 2014.

[13] Legislation targeting inBloom and similar companies ranged from lawsuits filed on behalf of New York City parents (eventually dismissed) to Oklahoma's House Bill 1989 (the Student Data Accessibility, Transparency and Accountability Act of 2013) to New York's Bill A8929, which prohibited the release of personally identifiable student data to third parties, and which passed 117-10 in the New York State Senate on 5 March 2014.

American discussions of privacy as a legal right can be traced to a single paper co-authored by Samuel Warren and (subsequent Associate Justice of the Supreme Court) Louis Brandeis in 1890; first appearing in the *Harvard Law Review,* 'The Right to Privacy' has been called 'the single most influential law review article ever published.'[14] The piece begins by reviewing freedoms with an established basis in tort law (e.g. freedom of the body, freedom of thought or conscience), but then goes on to argue that an intrusive mass media, and increasingly invasive technologies (like the telephone and 'instantaneous photographs'), have necessitated a more specific right to be left alone. As Warren and Brandeis search for a principle justifying such a right, they reject some obvious candidates (protection from physical assault, for example, or property law), and finally settle on a psychological, even spiritual, claim:

> The intensity and complexity of life, attendant upon advancing civilisation, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual. … Triviality [of social intercourse] destroys at once robustness of thought and delicacy of feeling. … The principle which protects [all] personal productions, is in reality … that of an inviolate personality.[15]

Less poetically: Warren and Brandeis understand the development of the individual as a fragile process, always at threat from the intrusions of everyday life. In order for a stable and healthy 'personality' to form, this process must remain 'inviolate'. Privacy, in short, is conceived ultimately as a necessary pre-condition for the formation of an autonomous person.[16]

---

[14] Harry Kalven, 'Privacy and Tort Law: Were Warren and Brandeis Wrong?' (1966) 31(2) Law and Contemporary Problems 326, 327.

[15] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy (The Implicit Made Explicit)' in Ferdinand Schoeman (ed), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press 1984) 75, 77, 82.

[16] David Rosen and Aaron Santesso, 'Inviolate Personality and the Literary Roots of the Right to Privacy' (2011) 23(1) Law and Literature 1.

It is not our brief here to trace the tortured legacy of Warren and Brandeis in both tort and constitutional law.[17] Suffice to say, however compelling their psychological insights, the claim about 'inviolate personality' has proven difficult to translate into practical applications. Indeed, in the most influential revision of 'The Right to Privacy', William Prosser (the leading expert on American tort law at mid-century) rejected their main insight altogether and identified the right to privacy with four overlapping, already-existing rights: freedom from intrusion, from the disclosure of private facts, from the presentation of one's character in a false light, and from the wrongful appropriation of one's name or image.[18] One can readily see how Prosser's revision (and its successors) have provided a firm basis for the attack on inBloom and other EdTech initiatives: the misuse of PII by school districts and third-party vendors may be interpreted as violating any or all of Prosser's four key principles. We would insist, however, that Warren and Brandeis are more useful for identifying the deeper threats latent in educational surveillance. Childhood, in the theory of personal development implicit in Warren and Brandeis, is the period when the self is least formed, and so most open to 'violation'. Thus a surveillance practice that attempts to influence the shaping of the self is likely to have lasting and possibly stunting effects. Unlike adults, moreover, children are ill-equipped to understand, let alone consent to, the pressures being exerted on them by, say, cameras in the classroom, or intensive testing-and-assessment regimes. Even staunch critics of inBloom et al sometimes miss the question of consent at the heart of these initiatives. Senator Markey, introducing the 'Do Not Track Kids Act', an amendment to the Children's Online Privacy Protection Act (COPPA) of 1998, presents the matter this way: 'Parents, not private companies, have

[17] It is easy to see why subsequent commentators would have trouble turning 'The Right to Privacy' into workable law, or even extracting a clear notion of the harm caused by privacy violations. For a discussion of this problem, see Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology* (Cornell University Press 1997) 4-15. The problem is central to the decision in *Doe v Chao* 540 US 614 (2004). In the words of Marc Rotenberg, director of the Electronic Privacy Information Center: 'Proving actual harm in a privacy case will remain very difficult.': US Senate Committee on Commerce, Science and Transportation, *Hearing: Online Personal Privacy Act* (S 2201 107th Cong, 2d sess, 25 April 2002) 'Prepared Statement of Marc Rotenberg' 36, 38.

[18] William L Prosser, 'Privacy' (1960) 48 California Law Review 383, 389.

the right to control personal information about their children. We should help student scholars make the grade, not help companies make a sale.'[19] By framing the question as an economic one, and as a matter of parental control of information, the 'Do Not Track Kids Act' is at once effective law, and a misrecognition of the most serious harm inflicted by tracking.

To this point, we have proceeded as if the definition of surveillance were self-evident; in fact, we have been relying on specific assumptions about surveillance and how it works. In a sentence, we would define it as 'the monitoring of human activities for the purposes of anticipating or influencing future events'. Within this definition, it should be perceived, we recognise two distinct activities: one watches other people in order to understand them, to gather information about them and anticipate their future actions, or—something quite different—one watches people in the hope that, if they *know* they are under watch, they will alter their behaviour in certain desired ways. We might call these two modes of surveillance 'empathetic' and 'coercive', respectively. Whereas the former mode, in its attempt to enter into the unguarded mind and uncover 'natural' behaviour, cannot announce its presence, and thus can take place anywhere, coercive surveillance typically occurs within controlled and delimited spaces, where the monitoring pressure can be strategically directed and selectively intensified. Perhaps counter-intuitively, the law is better at grappling with surveillance of the empathetic sort: surreptitious monitoring, once discovered, can be interpreted as an invasion of privacy in the first two ways identified by Prosser, and falls readily under now-acknowledged constitutional protections.[20] Coercive surveillance, on the other hand, announces its presence, making it clear that there should be no expectations of privacy under its gaze. Thus, we note, many of the responses to recent revelations of NSA dataveillance have been framed in

[19] Press release from Senator Edward Markey's office (14 January 2014) <www.markey.senate.gov/news/press-releases/markey-to-introduce-legislation-to-protect-student-privacy> accessed 21 November 2014.

[20] The US Supreme Court first recognized a constitutional right to privacy in *Griswold v Connecticut* 381 US 479 (1965). Acknowledging that the US Constitution never at any point mentions a right to privacy, the majority opinion, written by Justice William O Douglas located the right implicitly in the 'penumbras' and 'emanations' of already-existing protections.

Prosser's ready-made terms (intrusion, disclosure of private facts, etc.). Coercive surveillance, because it requires an awareness of its existence on the part of the observed, and is sometimes even entered into voluntarily (as when one enters a casino, say), is far harder to resist legally, even though, in Brandeisian terms, its effects are much deeper and longer lasting.

As should be clear, empathetic and coercive surveillance are completely distinct, one relying on the ignorance, the other on the awareness of those under watch. Nevertheless, when we look at surveillance in the classroom—or the rhetoric about surveillance in the classroom—we often see the categories getting blurred, and in knowingly prejudicial ways. In both Britain and America, for example, students and (especially) teachers have often felt coerced into certain pedagogical practices by the presence of CCTV cameras in the classroom: far from simply monitoring teaching, cameras inevitably change the way that teaching (and thus learning) happen.[21] The arguments promoting in-class use of CCTV, however, have overwhelmingly justified it (as in Bill Gates's TED talk) as a harmless form of empathetic data-gathering: it helps one better understand teachers as well as students. This blurring of categories can confer an operational advantage, as institutions camouflage practices under whichever model seems more legally convenient. Something of this bait-and-switch (going in the other direction) comes across in guidelines for 'The Appropriate and Effective Use of Security Technologies in U.S. Schools' published by the Department of Justice in 1999, just as these technologies were beginning to spread. The manual, concerned ostensibly with defending children against threats from without, begins entirely in the mode of empathetic surveillance: In 'Identifying the risks at a school …'

> A school's security staff must understand what it is trying to protect (people and/or high-value assets), who it is trying to protect against (the threats), and the general environment and constraints it must work within … . This understanding will allow a school to define its greatest

[21] Thus Mary Bousted, General Secretary of the UK's Association of Teachers and Lecturers has stated: 'We have major reservations about using CCTV to monitor staff. It is hard to see how teachers would act naturally if they knew they might be watched all the time on camera.' Quoted in: Jessica Shepherd, 'Someone to Watch Over You' *The Guardian* (London, 3 August 2009).

> and/or most likely risks … . From year to year … a school's security strategy will need revision because the world around it and the people inside it will always be changing … . A thorough understanding of employees, student profiles, and neighborhood characteristics will be necessary.[22]

The key words (*understand, define, revise, identify*) all belong to the world of inductive data-gathering, to the empathetic project of deriving information about other people. After only a few pages, however, the manual seems to discover the surveillance apparatus's coercive potential:

> The peace of mind of both students and faculty at a school can often be quickly enhanced by the installation of video cameras … . This change of attitude may result in even further-reaching effects on a campus than would be expected by the use of cameras alone … . A sense of safety and authority will directly influence people's opinions and impressions, which will ultimately contribute to the overall order maintenance of a facility.[23]

Almost imperceptibly, the language of 'understanding' and discovery is replaced by appeals to 'influence', authority and order; a recognition that the world 'is always changing' yields to the hope that something strong and stable can be created and 'maintained'. Flexible, knowledge-based protection, in essence, is supplanted by the coercive project of putting people in their proper places. And yet because the entire document is suffused with appeals for increased security from outside, the subsequent turn towards coercive surveillance is hard to detect. Empathy, in this case, 'covers' for coercion. And it is precisely under the guise of empathy that coercive technologies, with many more applications than security or innocuous data-gathering, have proliferated: in 1999, when this

[22] Mary W Green and others, 'The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies' National Institute of Justice Research Report (*US Department of Justice*, September 1999) 4.

[23] ibid 23.

report was released, 19 per cent of US schools used one or more cameras to monitor students; by 2009, 61 per cent did.[24]

But to what end? If we grant that the goal of coercive surveillance is to shape particular kinds of person, then what sort of person might an intensive regimen of educational monitoring produce? In their famous characterization of the 'millennials' (the generation comprising those born between 1982 and 2004), Neil Howe and William Strauss identify 'seven distinguishing traits' including 'confident' and 'achieving', but also 'conventional', 'sheltered', and 'pressured'.[25] Though these observations have been heavily criticized in some quarters, they have also struck a chord, entering into the public imagination; indeed, 71 per cent of American adults think of the millennials as 'selfish', and 65 per cent think of them as 'entitled'.[26] Described at one point by Howe and Strauss as 'the most watched-over generation in memory', the millennials are sometimes thought to have little interest in or even awareness of privacy, and are frequently condemned for their 'narcissistic and exhibitionist values'.[27] Although we doubt the validity of much generational stereotyping, and would question many of the attributes attached to the millennials, it is nonetheless worth reflecting on the way these widely commented-upon traits mirror the specific priorities of the classroom supervision and assessment this generation has

[24] Simone Robers and others, 'Indicators of School Crime and Safety (NCES 2012-002; NCJ 236021)' National Center for Education Statistics and Bureau of Justice Statistics (*US Department of Education* and *US Department of Justice*, February 2012) vii.

[25] Neil Howe and William Strauss, *Millennials Rising: The Next Great Generation* (Vintage Books 2000) 43-44. The two remaining characteristics are 'team oriented' and 'special'.

[26] Emily Ekins, '65% of Americans Say Millennials Are "Entitled": 58% of Millennials Agree' (*Reason-Rupe Public Opinion Survey*, August 2014) <http://reason.com/blog/2014/08/19/65-of-americans-say-millennials-are-ent3> accessed 21 November 2014. Also see, for example, Jean Twenge on millennial 'entitlement' and 'narcissism' in Jean M Twenge, *Generation Me* (Free Press 2007) and Jean M Twenge and W Keith Campbell, *The Narcissism Epidemic* (Free Press 2010); Joel Stein, 'Millennials: The ME ME ME Generation' *TIME* (New York, 20 May 2013) which begins 'Millennials are lazy, entitled narcissists.'

[27] Diane Mehta, 'New Survey Suggests Millennials Have No Idea What Privacy Means' (*Forbes*, 26 April 2013) <www.forbes.com/sites/dianemehta/2013/04/26/new-survey-suggests-millennials-have-no-idea-what-privacy-means> accessed 21 November 2014.

experienced (to a unique and unprecedented degree). It is only reasonable to expect that certain kinds of teaching will ultimately produce certain kinds of learners.

In the rhetoric that accompanies surveillance-dependent education reform, for example, the term 'personalized learning' is practically ubiquitous; thus one White House-produced report lauds the 'perfect personalization' made possible when innumerable 'bits of data [are] brought together to create a clear picture of a person to predict preferences and behaviours'. 'Real-time assessment [enables a] continuous improvement of course content'—a process the document labels 'personalizing education'.[28] Leaving aside the question of how traditional, face-to-face learning has come to be considered less 'personal' than a digital environment containing thousands, or even millions, of participants, we might focus on the meaning of the word 'person' implied by this rhetoric. It is in the nature of assessing and quantifying systems to privilege behaviours, and modes of learning, that can be assessed and quantified—and to de-emphasize the importance of modes less susceptible to easy measurement and monitoring. Thus a second White House report otherwise bullish on the potential of MOOCs sourly notes an objection, largely voiced by 'faculty in the humanities', that 'online courses may not be capable of inculcating in students … independent critical thinking', or the ability to 'formulate independent, original ideas, and arguments'.[29] In much the same way, but without drawing explicit links to the effects of educational surveillance, Howe and Strauss argue that millennials tend to 'avoid personal risks'; that they privilege 'group values' over 'independent' or 'individual' thought; that they are drawn to 'tangible results' and 'measurable, quantitative solutions'.[30] The eye of coercive surveillance does not observe neutrally; rather it strives constantly to render the objects of its gaze more visible and easily-comprehended. Surveillance-dependent education may indeed be more 'personal' in some ways—but this comes at the cost of reducing or simplifying what it means to be a person in the first place.

[28] Executive Office of the President (n 8) 7, 24.

[29] PCAST (n 7) 5.

[30] Howe and Strauss (n 25) 44, 223, 317.

The demise of inBloom suggests a growing awareness of the dangers in educational surveillance, and a canny appreciation in particular of the risks that accrue when responsibilities formerly the province of the government are outsourced to contractors whose motives are profit-oriented. Again, these dangers have typically been phrased in Prosserian, rather than (as we have attempted to do) Brandeisian terms. Nevertheless, the case of inBloom remains an outlier, with a preponderance of political (and, not coincidentally, financial) support on the other side, even for surveillance at its most invasive. Surprisingly, perhaps, in a political culture where entrenched partisan disagreement on virtually every topic has become the norm, educational surveillance has broad support from both Democrats and Republicans. Both parties are free to draw on the same neo-liberal assumptions. The presidential report on MOOCs surrenders decision-making powers ultimately to the Invisible Hand ('Let market forces decide which innovations in online teaching and learning are best'), and in much the same spirit, Secretary Duncan has dismissed problems encountered while implementing an online testing program as follows: 'There will be hurdles, there will be mistakes … but this is a business.'[31] A White Paper on education put out by (Republican) Mitt Romney's failed presidential campaign argued for 'standards' based on testing results, and 'encourage[d] market entry by [emphasizing] skill attainment instead of time spent in the classroom.'[32] Between this position and the stated priorities of the Democratic Obama administration there is little if any ideological distance: 'new educational technologies have the potential to … move away from measuring student progress merely

[31] PCAST (n 7) 6. Duncan's comments were delivered to the Writers Association seminar at Stanford University: Brooke Donald, 'At Stanford, Education Secretary Speaks on Preschool, Online Ed and Diversity' (*Stanford Report*, 2 May 2013) <http://news.stanford.edu/news/2013/may/arne-duncan-education-050313.html> accessed 21 November 2014.

[32] Romney for President, 'A Chance for Every Child: Mitt Romney's Plan for Restoring the Promise of American Education' (*Romney for President*, 23 May 2012) <www.mittromney.com> [site since taken down, archive version of the page available at <http://cdm16064.contentdm.oclc.org/cdm/ref/collection/p266901coll4/id/3980> accessed 21 November 2014]. For 'testing' and 'standards' see 3, 21; for 'skill attainment' see 4.

as time spent in a classroom, and toward a system that measures outcomes.'[33]

Rather than breaking down along the usual party lines, the debate over educational surveillance indicates a more entrenched class divide—one which we can see widening along practically every vector in Western Society. In an unguarded moment, the Presidential report on MOOCs suggests that 'low-cost training modules … might assist in providing the vocational skills that a twenty-first workforce needs.'[34] That workforce, it almost goes without saying, does not include the authors of the report, nor their children—a fact which brings us back, finally, to questions of regulation and the law. In the United States, the public educational system, ranging from kindergarten to large public universities like Berkeley or the University of Michigan, operates at the behest of federal, state and local legislatures, and has already (especially on the primary and secondary levels) succumbed to a regimen of intensive assessment and monitoring. The private educational system, however, especially in its upper echelons, where the training of the governing class is at stake, is far less subject to government oversight, and under fewer pressures to 'reform'. Thus Peter Salovey, president of Yale University, commenting on the future of MOOCs at his institution:

> A quality education represents a process of learning how to think, rather than the delivery of packets of information. I'm as excited about online technologies as anyone else, but I want to focus on [engaging] students with faculty in a process of teaching and learning [rather than] simply conveying packets of information and giving people merit badges for having viewed them.[35]

To translate: students who can afford an elite education will continue to enjoy the cost-ineffective, time-inefficient, personal 'teaching and learning' once thought crucial for the nurturing of autonomous, democratic citizens. For the remainder, a surveillance-enforced 'personalized' education, the goals of which are explicitly 'vocational', rather than directed towards a fuller personhood.

---

[33] PCAST (n 7) 3.

[34] PCAST (n 7) 5.

[35] Matthew Lloyd-Thomas, 'As Open Online Courses Evolve, Yale Remains Cautious' *Yale Daily News* (New Haven, 11 November 2013).

Whether this regime will succeed, however, is another question: as educators dealing with millennials on a daily basis, we would affirm that privacy is a topic of intense importance to the current generation of university students, who are profoundly clear-eyed about its benefits both for their education and for the development of their inner selves. That the generational descriptions offered by Howe and Strauss resemble the priorities of many contemporary educators may ultimately say more about the priorities of *their* generation (the Boomers, abetted by the X-ers), than anything essential about the cohort just entering adulthood. The targets of educational surveillance may well be stronger and more 'inviolate' than we often recognize.