UNIVERSITY USE OF BIG DATA SURVEILLANCE AND STUDENT PRIVACY

MACHAELLA REISMAN

ABSTRACT

As states cut funding for universities, universities in turn are seeking out new ways to diversify revenues. Concurrently, universities are struggling with losing students after their freshman year. Using student data and data analytics to predict which students are at risk of dropping out seems like an easy solution to the problem. Once identified through data mining, universities can target these at-risk students to retain them. In doing so, the university ensures it does not lose tuition from those at-risk students. However, universities fail to consider the privacy concerns that arise by bringing big data to college campuses.

Student autonomy and student choice suffer from the use of big data at a university. The use of big data then creates an environment of surveillance, which impacts students' learning. Further, big data impairs students' ability to innovate. Privacy violations contravene a university's mission and purpose; thus, privacy harms are something universities should care about.

Universities could self-regulate to protect student privacy, but this seems unlikely because universities have no incentive to stop data mining. Additionally, the current regulatory regime is unprepared to address the harms caused by big data. The shortcomings of the federal statutory regime are particularly salient when contrasted with other regimes, such as the California Consumer Privacy Act and the European Union's General Data Privacy Regulations. This Note proposes ways to fix the current regulatory regime, along with recommending new legislation that would provide privacy to students.

INTRODUCTION

Big data is everywhere today. One cannot go anywhere on the Internet without experiencing it in the form of targeted advertising.[1] For example, users will be tracked on 91% of the top one million websites.[2] As big data has swept across the commercial landscape, its proposed usefulness at predicting consumer behavior has become common knowledge. Given its widespread use in the business world, it should come as no surprise that colleges and universities have also decided to harness the power of data analytics. Universities struggle to retain students, and firms offer data analytics to help. However, the widespread use of big data on college campuses is creating more issues than it is solving.

First, big data is taking away student choice and the ability to develop autonomy. Second, the environment of surveillance created by the use of big data on college campuses may change the way that students learn. These changes may impair students' ability to become functioning members of democratic society. Third, big data takes away

[1] Nathalie Maréchal, *Targeted Advertising Is Ruining the Internet and Breaking the World*, VICE (Nov. 16, 2018 1:54 pm), https://www.vice.com/en_us/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world [https://perma.cc/KS72-5JBL].

[2] *Id.*

creative ability to innovate. Fourth, the surveillance environment pushes students to conform with the majority. Further, the use of big data to generate predictive algorithms often perpetuates previous biases, impinging on the rights of protected classes.

In 2016, Mount St. Mary's University in Maryland made the national news for its use of big data. The school's administrators decided to use big data analytics to track freshman students who were not happy at the school.[3] The school identified these students by administering a survey to freshmen and tracking whether they were going to on-campus events and attending classes.[4] The survey was given to students under the guise that it was a valuable tool to help students find what motivates them to succeed in school.[5] However, this was not the true motive behind the survey. The lack of transparency with the students became obvious after the revelation that the university president stated that he wanted to use the survey information to remove a number of students prior to the school's deadline to report enrollment data to the federal government.[6] By doing so, the school would artificially boost retention rates for the year by four to five percent.[7] In fact, the president is quoted to have said that professors "think of the students as cuddly bunnies, but you can't. You just have to drown the bunnies."[8] Without the use of big data, the school would have to wait until the first round of grades were released, roughly six weeks into the semester, to identify struggling students.[9] The fact that big data provides the ability to identify students to kick out before they have even finished their first six weeks of college is troubling.

Currently, the Family Educational Rights and Privacy Act ("FERPA") governs student privacy at universities.[10] FERPA works in conjunction with a set of Department of Education rules, which provide definitions and fill gaps.[11] However, this regulatory regime is inadequate to protect students from the use of big data on college campuses. Currently, FERPA does not regulate these uses of student data.[12] Further, exceptions to the consensual disclosure requirement allow universities to share student data with third parties.[13] On top of

[3] Susan Svrluga, *University President Allegedly Says Struggling Freshman Are Bunnies That Should Be Drowned*, WASH. POST (Jan. 19, 2016 7:01 PM), https://www.washingtonpost.com/news/grade-point/wp/2016/01/19/university-president-allegedly-says-struggling-freshmen-are-bunnies-that-should-be-drowned-that-a-glock-should-be-put-to-their-heads// [https://perma.cc/2UEB-L639].

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] 20 U.S.C. § 1232g (2018).

[11] *See* 34 C.F.R. § 99 (1996).

[12] *See* 34 C.F.R. § 99.3 (2012).

[13] 20 U.S.C. § 1232g(b)(4)(B) (2018).

the inadequate protections, this regulatory regime provides limited procedural rights to students in the event a university violates FERPA.[14] Ultimately, the decision to enforce a violation is up to the Department of Education.[15] The loopholes and lack of remedies leave students virtually helpless against universities' big data use.

The inadequacies of the federal privacy regime in protecting students are even more apparent when contrasted with state and European data privacy protections. For example, the California Consumer Privacy Act grants more rights to individuals to be free from big data processing.[16] The European Union's General Data Protection Regulations provides EU citizens the right to be free from automated decision-making, which lessens the ability to use big data.[17] These regimes highlight the types of protections that would empower students.

Part I discusses several troubling examples of big data surveillance at universities across the country, illustrating the power of big data predictions and the potential to be misused. Additionally, Part I explains why funding shortfalls leave so many universities with little choice but to implement big data practices.

Part II will discuss the harm to students that arise from the persistent use of big data at universities. This part will look at the underlying legal tradition that gives rise to Professor Julie Cohen's autonomy-based view of the importance of privacy.[18] It will also address the psychological benefits of privacy over surveillance, particularly relevant in the university setting. Next, it will compare the university setting to the employment setting and discuss the issues that have manifested there. Lastly, this part addresses forms of privacy models that universities may seek to implement, which are likely inadequate to remedy the harms being wrought by big data.

Part III considers non-regulatory measures that could be implemented to protect student privacy. Next, this part reviews the current framework of statutory privacy protections for college students and its shortcomings. Amendments to this statutory framework are then proposed, along with a discussion of potential rulemaking. This part concludes with a review of the protections offered by the California Consumer Privacy Act and the European Union's General Data Privacy Regulations.

[14] *See* 34 C.F.R. § 99, Sub. E. (1996).

[15] 34 C.F.R. § 99.60 (2017).

[16] CAL. CIV. CODE § 1798.100 (West 2020).

[17] General Data Protection Regulation 2016/679, art. 4, 2016 O.J. (L 119) 1, 33.

[18] *See generally* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subjects as Objects*, 52 STAN. L. REV. 1373, 1424 (2000).

I. THE APPEAL OF BIG DATA

Funding changes have left state universities anxious to retain students and concerned about budget shortfalls. Universities have turned to technology venders who offer a possible solution to both problems. The technology vendors gather students' location information and mine the resultant data. Universities may conclude that the benefits of this surveillance outweigh the costs. This part describes the perceived benefits. The next part explains costs to privacy and autonomy.

A. How Is Big Data Used on College Campuses?

Mount St. Mary's improper use of big data is not an isolated incident. The University of Arizona also uses big data in an attempt to identify struggling freshmen. A professor in the university's Eller College of Management led a research project at the university's Center for Business Intelligence and Analytics to analyze freshman students' ID card swipes to learn about students' routines and relationships, all under the guise of determining which students are most likely to return to campus after freshman year.[19]

Traditionally, when big data is used on college campuses, factors such as academic performance and demographic information are analyzed to determine the risk of dropping out.[20] However, the University of Arizona decided to take a different approach. The aforementioned professor pulled the timestamp and location information from each card swipe and analyzed it to determine social interactions.[21] Three years of freshman data were analyzed to create large network maps, allowing the professor and her team to determine not only which students interacted with each other, but for how long.[22] The interactions were monitored over a twelve-week period to determine the size of the students' social networks, whether the network grew or shrunk, and if the connections grew in strength.[23] The data was also analyzed to determine the students' routines, specifically if the student had a regular school-week routine.[24] The study determined that the less social interaction and routine, the more likely the student was to drop out.[25] While this research has not yet been incorporated into the university's predictive work, it likely will be soon.[26] The university next hopes to analyze students' Wi-Fi

[19] Alexis Blue, *Researcher Looks at 'Digital Traces' to Help Students*, UA NEWS (March 7, 2018), https://uanews.arizona.edu/story/researcher-looks-digital-traces-help-students/ [https://perma.cc/84P3-JE9R].

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

connections.[27] The university justified the ID swipe study's gathering of intensely personal data by noting that the data was anonymized and only shared with the individual student's advisor.[28] However, the fact that this information can be gathered at all serves to create a state of pervasive monitoring and surveillance on college campuses that engage in this sort of behavior.

Anonymization is not enough to protect privacy. In 2007, researchers from the University of Texas at Austin successfully de-anonymized Netflix data by comparing movie rankings of Netflix customers to movie rankings entered by individuals on Internet Movie Database ("IMDb").[29] The researchers demonstrated that the process of de-anonymization was not hard, nor did it require lots of data.[30] Using the rating information Netflix released, researchers referenced IMDb to find Netflix users who also entered movie rankings there.[31] Another example comes from the de-anonymization of medical records. In 2016, Australia released 2.9 million people's anonymized data, including medical billing records.[32] After the release, researchers from the University of Melbourne were able to identify people by comparing the released information to publicly available datasets.[33] The researchers learned the entire medical history of these individuals, all without consent.[34] These examples illustrate that anonymization is a fragile privacy protection at best.

Many schools are following a similar path. Virginia Commonwealth University implemented a program in 2019 to analyze students' Wi-Fi connectivity to determine whether students were attending class.[35] When a student logged into the university's Wi-Fi, the university recorded the timestamp and location information.[36] This data was then compared to the students' class times to determine if the students attended those classes.[37] Similarly, the University of North Carolina implemented a program for student athletes that utilizes Bluetooth

[27] *Id.*

[28] *Id.*

[29] Bruce Schneier, *Why 'Anonymous' Data Sometimes Isn't*, WIRED (Dec. 12, 2007, 9:00 PM), https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/ [https://perma.cc/BUC3-576G].

[30] *Id.*

[31] *Id.*

[32] Olivia Solon, *'Data is A Fingerprint': Why You Aren't as Anonymous as You Think Online*, THE GUARDIAN (July 13, 2018, 4:00 AM), https://www.theguardian.com/world/2018/jul/13/anonymous-browsing-data-medical-records-identity-privacy [https://perma.cc/FJ6H-Y85S].

[33] *Id.*

[34] *Id.*

[35] *VCU RAM Attend*, VIRGINIA COMMONWEALTH UNIVERSITY, https://studentsuccess.vcu.edu/ramattend/ [https://perma.cc/C63Z-T6KP] (last visited Jan. 19, 2020).

[36] *Id.*

[37] *Id.*

technology to determine class attendance.[38] The technology requires the student athletes to download an app which connects to a transmitted Bluetooth signal from the classroom to determine attendance.[39]

Yet another troubling example comes from the University of Texas at Dallas. In April of 2019, the student newspaper reported that the school would be installing Amazon Echo Dots in one of the residence halls to give students easy access to campus information.[40] The newspaper noted that if the pilot program worked, the Echo Dots would be installed in all residence halls.[41] Echo Dots already have concerning privacy implications. One Echo Dot user in London reported coming home to find his Echo Dot regurgitating previous commands, while another user in Germany randomly received approximately 1,700 audio files from someone else's Echo Dot, including enough information to find the inadvertent sender and his girlfriend's locations.[42] A user in Portland, Oregon discovered her Echo Dot sent a recording of a private conversation to one of her husband's employees.[43] These stories allow one to easily conjure up a scenario where conversations in student dorm rooms are sent to school employees. As discussed in Part II, this harms students by threatening their autonomy, which in turn threatens the ability to learn and make decisions.

B. Who Analyzes the Data?

While most universities have the capabilities to analyze gathered data, universities typically contract with third parties for this service. Colleges have a wide range of companies to choose from when selecting a big data analytics provider. The nonprofit Educause, which pushes for the use of information technology in higher education, plays a role in connecting universities with these providers.[44] At Educause's annual conference in 2019, more than 275 data analytics companies

[38] *See* Hannah McClellan, *UNC Tracking Student-Athlete Class Attendance Through Third-Party Beacon Tech*, THE DAILY TAR HEEL (Sept. 5, 2019, 12:28 AM), https://www.dailytarheel.com/article/2019/09/student-athlete-tracking [https://perma.cc/N3P7-RYRS].

[39] *Id.*

[40] Anjali Sundaram, *Amazon Echos to be Installed in Dorms*, THE MERCURY (April 15, 2019), https://utdmercury.com/amazon-echos-to-be-installed-in-dorms/ [https://perma.cc/BM2L-VKZY].

[41] *Id.*

[42] Dorian Lynskey, *'Alexa, Are You Invading My Privacy?' – The Dark Side of Our Voice Assistants*, THE GUARDIAN, (Oct. 9, 2019), https://www.theguardian.com/technology/2019/oct/09/alexa-are-you-invading-my-privacy-the-dark-side-of-our-voice-assistants [https://perma.cc/RA6N-XQFT].

[43] *Id.*

[44] *See generally* EDUCAUSE, https://www.educause.edu/ [https://perma.cc/W5V7-KSLP] (last visited April 5, 2021).

were present.[45] While attending the conference, university administrators had the opportunity to hear sales pitches from these companies and select those that appealed to their specific university.[46] Unsurprisingly, all the companies have a common theme: they claim that they will help save the university money and prevent student drop-out.[47] The shared vision of the companies is to create data profiles of students before they arrive on campus and even allow tracking after the student has graduated.[48] All companies claim efficiency as the payout for purchasing their products.[49] In fact, if a university were to buy all of the tools sold at the conference, the school could track just about every move of the students and professors, all justified by efficiency.[50]

By contracting with third-party vendors for services that process student data, universities create second level privacy concerns. A university that uses third-party services must ensure that when contracting with these companies, it knows exactly what the company is doing with the student data. A university should ensure that the third party is unable to sell student information. Additionally, universities should plan for possible data breaches with these outside vendors. Sending student information to a third party creates another opportunity for unauthorized access, such as an unauthorized party gaining access to students' personal information. The potential for harm to students far outweighs any benefit to universities. In the rush for big data in higher education, student privacy should not just be a peripheral concern.

C. Why Use Big Data?

As individual states cut funding for universities, universities are getting creative with ways to generate revenue; big data represents a way to diversify income streams for universities.[51] The primary purpose cited by universities for bringing big data to college campuses is the perennial problem of freshman retention rates and student success.[52] One reason freshman retention is an issue for universities is that it plays an important role in the way that colleges are ranked nationally and the university's overall reputation.[53] It presents challenges for the universities because freshmen who decide to leave

[45] Jeffrey R. Young, *How Tech Companies Are Selling Colleges on Mass Data Collection*, EDSURGE (Oct. 18, 2019), https://www.edsurge.com/amp/news/2019-10-18-how-tech-companies-are-selling-colleges-on-mass-data-collection [https://perma.cc/VP48-EKDQ].

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] Blue, *supra* note 19.

[53] *Id.*

college typically decide to do so within the first twelve weeks of a semester.[54] Thus, universities view big data as a way to monitor student behavior before grades are released for the semester, which is the traditional means of monitoring at-risk students.[55] For example, Educause pushes for the use of big data at universities as a means of understanding students to improve student recruiting, institutional efficiency, and cost effectiveness.[56] Educause and private data analytics companies market big data as a means to "save higher education."[57] These marketing efforts are working, as universities are buying into big data to save money.[58]

The push for big data also comes at a time when states have cut funding for higher education.[59] Concurrently, university enrollment is decreasing as a result of rising tuition costs and inability to get federal grants and loans.[60] These factors make it crucial for schools to retain current students in order to benefit the bottom line. While it is likely student success does play a role in incorporating big data into the university, monetary considerations are certainly a big factor. To be sure, universities are in a tough place financially to make up for money that they are no longer receiving due to these cuts in state funding and decreasing enrollment.[61] Given that rising tuition is a factor in the decrease in enrollment, the solution is not to continue increasing tuition to raise funds. However, while sympathetic to the universities' plight, revenue should not come at the expense of student privacy and autonomy and lead to the creation of an environment of surveillance on college campuses. Privacy will allow students to learn in ways that an environment of surveillance will not.

Universities have legitimate reasons for collecting and processing big data at their campuses. Student retention is important. However, as the Mount St. Mary's story illustrates, universities are able to cite admirable goals as the reasoning behind big data use while actually using the data for purposes that are not beneficial to the students. The story highlights both that universities' intentions do not always align

[54] *Id.*

[55] *Id.*

[56] Young, *supra* note 45.

[57] *Id.*

[58] *Id.*

[59] Jon Marcus, *Most Americans Don't Realize State Funding for Higher Ed Fell by Billions*, PBS (Feb. 26, 2019 12:20 PM), https://www.pbs.org/newshour/education/most-americans-dont-realize-state-funding-for-higher-ed-fell-by-billions [https://perma.cc/EBZ9-GW3D].

[60] *Id.*

[61] This is particularly true in light of COVID-19 and the impact the pandemic had on higher education. In fact, fall 2020 enrollment declined by 2.5%, which is twice as much as fall 2019. Madeline St. Amour, *Few Positives in Final Fall Enrollment Numbers*, INSIDE HIGHER ED (Feb. 28, 2020 4:42 PM), https://www.insidehighered.com/news/2020/12/17/final-fall-enrollment-numbers-show-pandemics-full-impact [https://perma.cc/LK3G-UP6G]. While not the focus of this Note, it will be interesting to see how the new consideration of the pandemic influences student privacy.

with the students' best interests and the discretion university administrators have in deciding how to use the data is an issue. Ultimately, this data gives administrators huge amounts of potentially personal data about students. The ability to determine students' routines and with whom a student spends time is a lot of power. Granting privacy rights to students will take this power out of the hands of administration. The next part explains why students should recover that power.

II. WHY PRIVACY MATTERS

Students need privacy. In particular, privacy facilitates the development of autonomy. The benefits of autonomy include non-conformity, self-governance, and innovation. This part shows how surveillance impairs autonomy. The harm caused by surveillance is not just felt in the university setting. The use of artificial intelligence in hiring decisions highlights additional harms that will arise from the use of big data. Moreover, pay-for-privacy models will not fix the privacy issues at universities.

A. The Need for Autonomy

The university setting highlights the impact of technology in privacy. College freshmen embark on a journey not just to learn in academic classroom settings, but also to get involved in on-campus organizations and activities to discover hidden passions and gain fulfillment. As a result, college is a formative time in an individual's life. Pervasive surveillance of college students is not a simply an annoyance. In fact, the form of surveillance described in Part I can have long term impacts on students and society. In the United States, we value autonomy and the freedom to make our own choices. However, as Julie Cohen notes, "Autonomous individuals do not spring full-blown from the womb."[62] A crucial feature of autonomy is the ability to process information and use that information to make determinations about the world.[63] By default, autonomy is the independence to think for oneself, free of outside influence.[64] Thus, autonomy is dependent on the environment in which it is fostered.[65] The ability to think autonomously is necessary to yield productive members of society. In fact, research has shown autonomy to be a crucial factor in workplace productivity but requires development to exist.[66] An environment which fosters autonomy is one in which

[62] Cohen, *supra* note 18, at 1424.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] *Id.* (citing Steve Williams, *An Organizational Model of Choice: A Theoretical Analysis Differentiating Choice, Personal Control, and Self-Determination*, 124 GENETIC SOC. & GEN. PSYCH. MONOGRAPHS 465 (1998)).

individuals are free to deliberately and thoughtfully construct themselves.[67]

The idea that autonomy is important in shaping society is not a new one. America's founders were ideologically influenced by John Locke, who viewed laws as a way to preserve individual liberties.[68] Locke also believed that personal freedom was needed for "even that minimum development of his natural faculties."[69] Locke's beliefs regarding personal freedom are reflected in the Declaration of Independence,[70] as well as the Bill of Rights.[71] Autonomy has thus been a key part of political theory since the inception of the United States.[72] Thus, "autonomy comports with important values concerning the fair and just treatment of individuals within society."[73] Philosopher Immanuel Kant also influenced American philosophical tradition with beliefs that still play an important role today. Kant's philosophy emphasizes respect for dignity of persons and requires commitment to not only egalitarianism principles, but to egalitarian practice as well.[74] Thus, the importance of autonomy for human development was understood by the Framers and those whose legal theories provided the basic rationales for our constitutional system of government.

1. Psychological Justifications for Autonomy

Today, principles of psychology shed light on why autonomy is essential for humans.[75] First, research shows that a positive relationship exists between individual choice and achievement of goals.[76] Professor Bruce Winick provides the example of patient response to medical treatment to illustrate the health benefit from buy-in.[77] Patients who are not allowed to participate in treatment decisions tend to fail to comply with their physicians' medical advice.[78] Conversely, when patients have the ability to choose between alternative treatments, there is a greater likelihood of successful treatment.[79] Professor Winick notes that this positive relationship is applicable in the educational context.[80] Conscious goal-setting by an

[67] *Id.*

[68] Bruce Winick, *On Autonomy: Legal and Psychological Perspectives*, 37 VILL. L. R. 1705, 1708 (1992).

[69] *Id.* (quoting Isaiah Berlin, FOUR ESSAYS ON LIBERTY 124 (1969)).

[70] *Id.* (citing Garrett W. Shelton, THE POLITICAL PHILOSOPHY OF THOMAS JEFFERSON 9, 12, 42-45 (1991)).

[71] *Id.* at 1710.

[72] *Id.* at 1711.

[73] Cohen, *supra* note 18, at 1423.

[74] *Id.* (citing Immanuel Kant, THE METAPHYSICS OF MORALS 73-74, 231-32 (Mary Gregor ed. & trans. 1996 and John Rawls, A THEORY OF JUSTICE (rev. ed.) (1999)).

[75] Winick, *supra* note 68, at 1756.

[76] *Id.* at 1757.

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *Id.* at 1758.

individual is indispensable to achieving that goal, which is directly applicable in the educational context.[81] Thus, individual goal-setting in the context of education is crucial to achieving those educational goals.[82] This theory is backed by empirical research, which found that when a student made a choice about education, the student worked "'harder, faster, and react[ed] more positively to the situation than when they [were] unable to make such choices.'"[83] When schools utilize big data to push students in the way that the school wishes the students go, the school acts contrary to this psychological theory, reducing the students' ability to set and achieve their own academic goals and perhaps undermining educational goals.

The ability to make choices and set goals gives an individual a sense of competence, which is considered a prerequisite for sound psychological health.[84] Psychologist Edward Deci argues that self-determination is an essential human need, and studies show that taking away individual choice decreases motivation and a desire to learn.[85] In fact, the ability to choose is a necessary intrinsic motivation.[86] By utilizing big data in the educational context, universities are undermining autonomy to make educational choices, which in turn is taking away students' sense of competence. Without this, the environment of surveillance on university campuses is undermining students' psychological health.

Creating an environment in which autonomy can grow provides tangible benefits to students at institutions of higher education. These benefits are something that administrators should value as well, as these benefits are part of a university's mission. Autonomy as unmonitored choice creates diversity in speech and behavior, including political and intellectual speech or associations that may be unpopular.[87] However, the ability to make unmonitored choices goes beyond these behaviors.[88] Individuals experiment with preferences of every type of behavior that a person may exhibit.[89] This process of learning is vital to formulating the self, particularly for college-aged individuals.[90] Without privacy, there is no opportunity for individuals to engage in "meaningful reflection, conversation, and debate about

[81] *Id.* (citing Albert Bandura, SOCIAL FOUNDATIONS OF THOUGHT AND ACTION: A SOCIAL COGNITIVE THEORY, 338, 469 (1986)).

[82] *Id.* at 1759.

[83] *Id.* at 1762 (quoting Thomas A. Brigham, *Some Effects of Choice on Academic Performance*, in CHOICE AND PERCEIVED CONTROL 131, 140 (Lawrence C. Perlmuter & Richard A. Monty eds., 1979)).

[84] *Id.* at 1765 (citing Edwin L. Deci & Richard M. Ryan, *The Empirical Exploration of Intrinsic Motivational Processes*, in 13 ADVANCES IN EXPERIMENTAL SOC. PSYCHOL. 39, 61 (1980)).

[85] *See generally* Edward L. Deci, INTRINSIC MOTIVATION (1975).

[86] *Id.*

[87] Cohen, *supra* note 18, at 1425.

[88] *Id.*

[89] *Id.*

[90] *Id.*

the grounds for embracing, escaping, and modifying particular identities."[91] It is helpful to compare the benefits of privacy in information with privacy rights from physical visual surveillance, as discussed in the next section.[92]

2. *Surveillance Harms*

Pervasive surveillance on college campuses injures students in ways that exceed the invasion of students' location information. The value in being free from surveillance in physical spaces means that there is a space in which an individual may be unobserved and provide a place to be free from society.[93] Invading this form of privacy crosses an emotional boundary.[94] These same values apply with equal force to privacy in information, which is also violated by pervasive surveillance.[95] The problem with pervasive surveillance is that it not only dissolves boundaries, but also collects information from any student activity that generates records.[96] In turn, the aggregation of information collection paints a picture of the students' lives that includes intimate details.[97] This form of surveillance does not turn on whether the students are in private or public, making it far more pervasive than visual surveillance.[98]

An environment of surveillance, which eliminates privacy, changes the way students will learn.[99] Not only will students learn differently, but "the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior."[100] In fact, the field of cognitive psychology produced research that indicates a lack of privacy makes people less likely to experiment or seek out help.[101] The result is that students will be inclined to make choices that are more mainstream and less out-of-the-box, as every move will be surveilled.[102] The out-of-the-box thinkers will slowly shift towards mainstream ideas and a valuable portion of society will be lost as result.[103]

A trend toward conformity would cut against American legal tradition, as out-of-the-box thinkers are responsible for major reforms throughout history.[104] Without privacy, pervasive surveillance will

[91] Anita Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 754-55 (1999).
[92] Cohen, *supra* note 18, at 1425.
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.* at 1425-26.
[98] *Id.*
[99] *Id.* at 1426.
[100] *Id.*
[101] *See generally* Stuart A. Karabenick & John R. Knapp, *Effects of Computer Privacy on Help-Seeking*, 18 J. APPLIED SOC. PSYCHOL. 461 (1988).
[102] Cohen, *supra* note 18, at 1426.
[103] *Id.*
[104] *Id.*

dampen any desire for thinking that does not accord with the mainstream.[105] The reason privacy is so important is that it will allow for autonomy, which allows individuals to make choices about themselves—even when open to outside influence.[106] The ability to make choices surrounded by others is an essential element of autonomy, as no one makes decisions without the influence of outside factors.[107] The exercise of autonomy allows individuals to shape their lives by the choices they make.[108] However, threats that influence a person's "reasoning process" shape the way decisions are made and, thus, dictate autonomy.[109] An influence that takes over the way a person thinks and produces a different outcome changes the way learning occurs.[110]

The ability to think outside the box and make individualized choices despite outside influence is particularly important within the university context. Students are barraged with information and choices in college, both personal and educational. Students may take a required class within their major and do poorly or hate it, prompting a decision about whether they should change their major. Or a student may join an on-campus organization that causes the student to reflect on personal beliefs. Within an environment of surveillance, these formative choices may no longer occur. However, with privacy and personal space, students can reason through choices that must be made while in college, all while learning in a way that produces capable individuals who can contribute to society.

A case from the Court of Appeals of Georgia provides a useful illustration of how surveillance changes behavior.[111] *Anderson v. Mergenhagen* involved the harassment of a wife.[112] The wife argued that for almost two years the boyfriend of her husband's ex-wife followed her while taking pictures, making gestures, and ensuring the wife knew he was there.[113] This surveillance caused the new wife to change her behavior, as she was too scared to even go to her community pool.[114] Another such incident led the new wife to cut short her walks with her children, as he would follow her in his car taking pictures.[115] These incidents occurred monthly, consistently requiring the new wife to change her routines and behavior to avoid being

[105] *Id.*

[106] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1655 (1999).

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.* at 1656.

[111] Anderson v. Mergenhagen, 642 S.E.2d 105 (Ga. Ct. App. 2007).

[112] *Id.* at 107.

[113] *Id.*

[114] *Id.* at 107-08.

[115] *Id.*

surveilled by the ex-wife's boyfriend.[116] On appeal, the court held that the lower court incorrectly granted summary judgment in favor of defendant.[117] The court noted that the right to privacy is an essential and fundamental principle.[118] Moreover, the court explained that the tort of intrusion upon seclusion requires an unreasonable intrusion that would be offensive to a reasonable person.[119] The court held that even a relatively harmless activity can become tortious with repetition, especially once the repeated activity becomes a substantial burden to a plaintiff's existence.[120] Thus, even surveillance while in public can be tortious when it is enough to repeatedly frighten the wife and cause her to change her behavior.[121] While an extreme example, the case demonstrates that persistent surveillance leads individuals to change their behaviors.

B. Benefits of Autonomy and Privacy

Autonomy and privacy produce distinct benefits. First, autonomy and privacy lead to self-governance. Self-governance is necessary for democracy. Thus, autonomy at universities is required to further democracy. A second benefit of autonomy and privacy is non-conformity. Without surveillance, individuals are free to think without the pressure of following the majority. Lastly, innovation is a benefit of autonomy and privacy. Without big data, universities will create an environment allowing students to innovate.

1. Self-Governance

Self-governance is a distinct benefit of autonomy, which is the backbone of democracy.[122] If individuals are to meaningfully participate in democracy, whether that be politically, socially, or economically, independent choice must occur.[123] However, constant surveillance chills the political experimentation that is needed to form political preferences.[124] For meaningful discussion in democracy, individuals must be able to find personal definitions of self in private and "(if one desires) to keep distinct social, commercial, and political associations separate from one another."[125] To further the goals of democracy, individuals must be capable of self-governance.[126] However, colleges and universities that engage in surveillance

[116] *Id.*
[117] *Id.*
[118] *Id.*
[119] *Id.* at 109.
[120] *Id.* at 110.
[121] *Id.*
[122] Cohen, *supra* note 18, at 1426.
[123] *Id.*
[124] *Id.*
[125] *Id.* at 1426-27.
[126] *Id.*

undermine society as a whole and, specifically, democracy by impairing students' ability to learn self-governance.[127]

The impact of surveillance on democratic citizens is shown through examination of the economic and political institutions that are part of democracy.[128] Practices of democratic citizens include voting and public debate of issues, which are learned traits of citizens.[129] Capacity for citizenship is shaped by political and economic institutions in the way that rhythms and norms are learned traits that are internalized to become behavior.[130] As surveillance becomes an ordinary feature, it gains even greater power.[131] The power of surveillance denies individuals the opportunity to develop habits of mind that are required for critical citizenship in a democratic society.[132] By creating an environment of surveillance with little privacy for students, colleges are reducing space for students to think critically. Affording students privacy provides students with opportunities to learn self-governance and, ultimately, contribute to democracy. Without privacy, over time, "[t]he liberal democratic society will cease to be a realistic aspiration unless serious attention is given to the conditions that produce (aspiring) liberal selves."[133] Critical thinking is not only important for self-governance, but also necessary to allow space for the minority to express an opinion. As shown in the next section, minority groups are critical for democratic problem-solving.

2. *Non-Conformity*

Julie Cohen is not alone in the belief that surveillance impacts the way society learns. As Professor Neil Richards explains, surveillance threatens the value of "intellectual privacy."[134] Intellectual privacy is a theory based on the belief that "new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing."[135] Crucial to the theory is the idea that the ability to think freely is completely necessary for a free society.[136] When activities that generate beliefs and ideas are surveilled, the generation of ideas is negatively impacted.[137] "[I]ntellectual diversity and eccentric individuality" need to be protected.[138] When there is surveillance,

[127] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013).

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *Id.* at 1916.

[132] *Id.* at 1918.

[133] *Id.*

[134] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1945 (2013).

[135] *Id.* at 1946.

[136] *Id.*

[137] *Id.*

[138] *Id.*

individuals are more likely to follow the mainstream.[139] Surveillance deters activity that may be viewed as deviant.[140]

Privacy can shield belief-forming activities from surveillance so that the exchange of ideas is fostered.[141] This justification of privacy has its roots in First Amendment doctrine and the concerns of a chilling effect.[142] The justification is that if the formation of beliefs and individuality is important under the First Amendment, surveillance that impacts the same sort of behavior should be frowned upon.[143]

The chilling effects recognized under the First Amendment have roots in social psychology. Professor Margot Kaminski and attorney Shane Witnov explain the interplay between the negative impact of surveillance and its chilling effect, formulating what they call the "conforming effect."[144] While a chilling effect may be a product of surveillance, they believe the more subtle and pernicious effect is the conforming effect, which affects decision-making without individuals' awareness of its influence.[145] Social psychology shows that group behavior strongly influences individual behavior,[146] with long-lasting effect on beliefs.[147] Further, behavior can be influenced with just a suggestion that it is being observed[148] and often without realization that behavior is influenced.[149] The impact of surveillance can also be so profound as to influence the decision on what to read or whether to explore a new topic.[150] Thus, the conforming effect requires no awareness by the individual that they are being influenced.[151]

There are two identified types of conforming behavior.[152] Private conformity occurs when other people cause an individual to change personal behavior to conform to group behavior, while public conformity is when the person acts like the rest of the group but does not change beliefs to align with the group.[153] For example, researchers

[139] *Id.* at 1948.

[140] *Id.*

[141] *Id.* at 1950.

[142] *Id.*

[143] *Id.*

[144] Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 483 (2015).

[145] *Id.*

[146] *Id.* (citing Gregory S. Berns et al., *Neurobiological Correlates of Social Conformity and Independence During Mental Rotation*, 58 BIOLOGICAL PSYCHIATRY 245, 245 (2005)).

[147] *Id.* (citing J.H. Rohrer et al., *The Stability of Autokinetic Judgments*, 49 J. ABNORMAL SOC. PSYCHOL. 595, 597 (1954)).

[148] *Id.* (citing Aaron M. Watson et al., *When Big Brother Is Watching: Goal Orientation Shapes Reactions to Electronic Monitoring During Online Training*, 98 J. APPLIED PSYCHOL. 642, 643-44, 650 (2013)).

[149] *Id.* (citing Solomon E. Asch, *Effects of Group Pressure Upon the Modification and Distortion of Judgments*, in GROUPS, LEADERSHIP AND MEN (Harold Guetzkow ed., 1951), reprinted in DOCUMENTS OF GESTALT PSYCHOLOGY 222, 223-28 (Mary Henle ed., 1961)).

[150] *Id.* at 484.

[151] *Id.*

[152] *Id.* at 487.

[153] *Id.*

conducted a study of alcohol use and perception on a college campus.[154] The results found that, on average, males students were far less comfortable with alcohol use on campus than students perceived the average student to be.[155] The actual comfort level with alcohol on campus was not as high as students believed it to be.[156] However, as a result of the perception that comfort level was higher, the students tended to shift thoughts toward that perceived norm over time.[157] This study illustrates that even the perception of majority norms forces conformity with those norms.[158]

Another example points more directly to the effects of surveillance on conformity. In the 1970s, in an experiment conducted at University of California Los Angeles, researchers asked students to give a short talk on marijuana possession and whether small quantities should be a misdemeanor and large quantities a felony.[159] All students were told they would be videotaped, with about half the students told that copies would be given to law enforcement.[160] Of those told that tapes would be given to law enforcement, only a small subset was actually taped.[161] The others were told that the camera was broken and would instead just be voice recorded, which would not be shared with law enforcement.[162] Prior to the talk, the students were split evenly about agreement with the statement.[163] After the experiment, however, only 44%of those in the video surveillance group advocated for legalization of marijuana, yet 73% of those in the non-surveillance group advocated for it.[164] Even those who were first told they would be videotaped and later told they would not be videotaped remained influenced by the threat of surveillance.[165] The researchers concluded that the threat of surveillance was a powerful behavioral influence, even when the threat was not realized.[166] Additionally, the students, whether surveilled or not, reported honest performance and stated that surveillance did not influence statements.[167] However, the results pointed to strong conformance with knowledge of surveillance.[168] The

[154] *Id.* at 488 (citing Deborah A. Prentice & Dale T. Miller, *Pluralistic Ignorance and the Perpetuation of Social Norms by Unwitting Actors*, in 28 ADVANCES IN EXPERIMENTAL SOC. PSYCHOL. 161, 172-75 (1996)).

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *Id.* at 491 (citing Gregory L. White & Philip G. Zimbardo, *The Effects of Threat of Surveillance and Actual Surveillance on Expressed Opinions Towards Marijuana*, 111 J. SOC. PSYCHOL. 49-50 (1980)).

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] *Id.* at 492.

[164] *Id.*

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] *Id.*

result was that political speech about marijuana legalization was chilled by mere threat of surveillance.[169]

The chilling of activity is just the beginning of the harms wrought by the conforming effect.[170] The conforming effect greatly influences the undecided individual.[171] This is particularly troubling in the context of big data surveillance by colleges. While learning in college, students may be undecided on any number of issues, political or social. The influence of surveillance on an undecided college student means that the student will trend toward the conforming behavior or beliefs of the majority. The more uncertain the student is, the more susceptible to influence that person is.[172] The powerful impact of surveillance is detrimental to individual thought at such a formative time in a person's life. Additionally, surveillance can increase anxiety and unease, which in turn impacts cognitive abilities.[173] The aforementioned University of California at Los Angeles study reported that the students who were told they were being surveilled scored higher in anxiety and inhabitation factors.[174]

Yet another harm of surveillance is that it also weakens the influence of minority ideas.[175] Minority influence requires critical thought and creative thinking and, even when ultimately unsupported, contributes to finding new solutions to problems.[176] However, a 2014 Pew Research Center study found that people are less likely to speak up on issues in public if they believe they are in the minority.[177] Surveillance makes people feel more sensitive about being in the minority and, in turn, more reluctant to share opinions.[178] An environment of surveillance makes it much harder to commit to the minority position.[179] These harms can be felt by college students as they make choices about who they are and what they believe in while in college. Privacy would allow students to be free from the conforming effect and give students the ability to be in the minority, if they so choose, without fear of the majority. Privacy would also allow students to make the decisions without additional anxiety or unease, which is extremely beneficial to students.

[169] *Id.* at 499.

[170] *Id.* at 499-500.

[171] *Id.* at 500.

[172] *Id.*

[173] *Id.* at 501.

[174] *Id.*

[175] *Id.* at 506.

[176] *Id.*

[177] *Id.* at 507 (citing Keith N. Hampton et al., *Social Media and the 'Spiral of Silence*,' PEW RES. CTR. 8, 23 (2013)).

[178] *Id.*

[179] *Id.*

3. *Innovation*

Privacy promotes innovation.[180] True innovation requires, "the capacity for critical perspective on one's environment and . . . is not only about independence of mind."[181] Surveillance creates an environment that lacks the freedom and space needed for innovation.[182] Innovation requires innovative practice, and "innovative practice is not linear."[183] In fact, innovation is "multidirectional, stochastic, [and] full of feedback loops."[184] Outside influences and challenges affect feedback loops, while also providing opportunities for innovation to happen.[185] However, circumstances that create "intellectual regimentation" and "restrict[] the freedom to tinker" create an environment that diminishes innovative chance.[186] True innovation requires not only space, but also the ability for variable behavior.[187] Variable behavior combined with new ideas and serendipity creates innovation, which flourishes when there is both "intellectual and material breathing room to experiment with them."[188] Conversely, innovation does not occur in environments of intellectual restriction with no room for self-determination.[189]

Environments with pervasive surveillance that influence behavior do not allow the freedom to tinker, which is necessary for innovation.[190] Pervasive surveillance chills innovative activity, and Julie Cohen believes that any thought to the contrary is "simply silly."[191] The idea that innovation could exist in an environment of pervasive surveillance requires belief in a construct of "the liberal subject, who can separate the act of creation from the fact of surveillance."[192] Individuals do not respond to surveillance like this, and instead surveillance molds individuals behaviors.[193] This is comparable to the subtle process of behavioral advertising, which pushes consumers towards products in a highly personalized way.[194] Likewise, search engines and social media push citizens towards political inclinations by conforming the information environment to personalized political and ideological beliefs.[195] In the same way, innovation is subtly

[180] Cohen, *supra* note 127, at 1918.

[181] *Id.*

[182] *Id.*

[183] *Id.* at 1919.

[184] *Id.* at 1919-20 (quoting Brett M. Frischmann, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 272 (2012)).

[185] *Id.* at 1920.

[186] *Id.*

[187] *Id.* at 1918.

[188] *Id.* at 1920.

[189] *Id.*

[190] *Id.*

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] *Id.* at 1916.

[195] *Id.* at 1917.

influenced by surveillance. Thus, with privacy, people may develop self-determination, and there will be room for innovation.[196]

Universities should value, appreciate, and create space for innovation. Traditionally, universities are places where students have opportunities for hands-on experiences that allow for innovation and invention. Innovative ideas by students and professors at universities lead to prestige and respect from the outside world for that university. With this goal in mind, it would behoove university administration to provide privacy and space to students to promote innovation. An environment of surveillance is not one in which students are given the tools to innovate and provide new and fresh ideas. Promoting privacy will ultimately serve the desired goal of promoting innovation on university campuses. This space to tinker, as Cohen puts it, will allow students to try and fail without fear and encourage them to try again if they do.

Surveillance masquerading as big data attempts to call itself innovative. It is not.[197] Big data is a means to find patterns within datasets to provide predictive information.[198] While it can be used scientifically, it is used to analyze the physical and behavioral data of individuals.[199] Individuals' judgments and preferences are predicted in such a way that it shapes individuals' preferences.[200] Using big data in this way not only surveils individuals but also shapes their needs and preferences and completely undercuts the autonomy of self-choice. The environment created by big data surveillance does not allow for independent thought and, over time, will completely eliminate innovation.[201] Privacy is needed to promote true innovation. Thus, when privacy is allowed, "tinkering and behavioral variation" needed for innovation will emerge and innovation will thrive.[202]

Admittedly, schools have occasionally used big data surveillance to good ends. A report by the New America Foundation highlights some of the promise of big data in higher education.[203] Specifically, big data surveillance can be used to implement systems that alert universities as early as possible of students at risk of dropping out in order to provide targeted advising.[204] Another promise is the use of adaptive learning, which adapts to the specific needs of the individual

[196] *Id.* at 1920.

[197] *Id.* at 1918-19.

[198] *Id.* at 1920.

[199] *Id.* at 1921.

[200] *Id.* at 1925.

[201] *Id.* at 1926.

[202] *Id.* at 1927.

[203] Manuela Ekowow & Iris Palmer, *The Promise and Peril of Predictive Analytics in Higher Education: A Landscape Analysis*, NEW AMERICA (Oct. 24, 2016), https://na-production.s3.amazonaws.com/documents/Promise-and-Peril_4.pdf [https://perma.cc/DAP2-E3GN].

[204] *Id.*

student.[205] Yet another promise is the ability to increase enrollment yield by using the characteristics of students who have enrolled in the past to determine the chances that a potential student will enroll.[206] The report also notes that big data can be used positively to tailor financial aid in order to maximize the chances that students enroll.[207]

However, in addition to privacy concerns, the report mentions several challenges in using big data.[208] The first is that the models used can discriminate based on age, race, gender, and socioeconomic factors, as these factors are central to the analysis and will mirror the past discrimination in the dataset.[209] This means that colleges that use big data for predictive analytics regarding admissions run the risk of disfavoring minority students.[210] Additionally, there is the risk that the algorithms point towards recruiting wealthier students over low-income students because wealthier students have historically enrolled at the school.[211] Another challenge is that colleges using big data are not transparent about its use, but they should be.[212] Transparency includes being open about the quality of the data being used and any potential for bias.[213] Transparency also extends to the outside vendors that colleges contract with, so colleges should choose vendors carefully.[214]

C. *Problems With the Use of AI in Employment*

We can better understand the harms of using big data in educational decisions by comparing the use of big data in hiring decisions. This comparison reveals the potential for biased decision-making when hiring based on algorithm recommendations. In fact, Amazon uncovered that its recruiting algorithm was biased against women.[215] The company deployed a team in 2014 with the task of building computer programs to create an automated process for recruiting talent.[216] The program utilized artificial intelligence to generate scores for job candidates that ranged from one to five stars.[217] A year into the development, the company realized that the system

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] *Id.*

[214] *Id.*

[215] Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 9, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/K7CY-A7B8].

[216] *Id.*

[217] *Id.*

was not rating candidates for technical jobs, such as software development, in a gender-neutral way.[218] The models were generated based on Amazon's past applicants over a ten-year period and, given the male dominance of the tech industry, those successful applicants were mainly men.[219] The system penalized resumes that included the word "women's," thus downgrading graduates of all-women's colleges.[220]

Another iteration of Amazon's AI program was being developed around the same time to search the internet for candidates worth recruiting, focusing on job function and location.[221] Amazon again discovered that the system favored candidates who used language that was more commonly found on male resumes, such as "executed" and "captured."[222] Additional problems with the system meant that unqualified candidates were recommended for jobs over their more qualified counterparts.[223] Amazon is not the only company to seek a way to utilize AI for recruiting and hiring. Big names such as Unilever, Hilton, and Goldman Sachs all use AI in hiring.[224]

Professor Pauline Kim dissects the process behind the use of algorithms in hiring decisions.[225] Companies use an applicant screening tool, which is often automated software provided by a third party, that analyzes the data from each applicant and decides which candidate deserves to make it to the next step.[226] The software utilizes an algorithm to predict which applicants are most capable of performing the described job.[227] The software creates this algorithm by taking vast quantities of data to analyze and find any existing statistical relationships between the given variables.[228] Then, the discovered relationships are used to build predictive models to be applied in future cases.[229] The predictive model, in the manner used by big data analytics scientists, can not only identify patterns but can also infer characteristics.[230] Ultimately, recruiting and hiring algorithms observe correlations to predict future human behavior.[231]

When relying on algorithms for hiring and recruiting, the first risk is that the employer may consciously rely on protected characteristics

[218] *Id.*

[219] *Id.*

[220] *Id.*

[221] *Id.*

[222] *Id.*

[223] *Id.*

[224] *Id.*

[225] *See generally* Pauline T. Kim, *Big Data and Artificial Intelligence: New Challenges for Workplace Equality*, 57 U. LOUISVILLE L. REV. 313 (2019).

[226] *Id.* at 317.

[227] *Id.*

[228] *Id.*

[229] *Id.*

[230] *Id.*

[231] *Id.*

in choosing who may see a job posting.[232] For example, if any employer uses demographic-targeting variables, a certain gender or age group could be chosen when deciding who sees the advertisement.[233] This form of targeting can occur even if the employer does not expressly choose to discriminate this way.[234] An employer may choose an attribute like "young professional" that indirectly corresponds with age.[235] Screening and scoring algorithms can appear neutral but actually rely on a proxy attribute that causes implicit bias, such as zip codes.[236] This may seem like a neutral attribute, but in certain cities place of residence may closely correspond with race.[237] Additionally, an algorithm can produce biased results if it is made from biased data.[238] If built from a biased dataset, biased results occur.[239] If the algorithm bases hiring decisions on comparisons with current employees, and the current employee makeup has few women, then the algorithm will simply recreate that.[240] Thus, predictive models are only as good as the existing dataset that the model is built upon.[241]

Allowing algorithms based on protected classes led to trouble for the company Roomates.com, LLC.[242] The company operates a website that allows people to connect with others who are renting out rooms.[243] In order to use the services, an individual must create a profile and answer certain questions.[244] A section of the questions addressed sex and sexual orientation.[245] The user was also required to select which sex and sexual preference they would prefer in a roommate.[246] The Fair Housing Council sued, alleging that by requiring these answers, there was an intent to discriminate based on the answer.[247] The Ninth Circuit determined that Roommates.com designed its search systems to limit listings that subscribers view based on sex and sexual orientation.[248] Ultimately, the court found that the company could be held liable for using the questions and remanded to the lower court to determine the legality of asking the questions.[249]

[232] *Id.*

[233] *Id.*

[234] *Id.* at 319.

[235] *Id.*

[236] *Id.* at 320.

[237] *Id.*

[238] *Id.*

[239] *Id.*

[240] *Id.*

[241] *Id.*

[242] *See* Fair Hous. Council of San Fernando Valley v. Roomates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

[243] *Id.* at 1161.

[244] *Id.*

[245] *Id.*

[246] *Id.*

[247] *Id.* at 1164.

[248] *Id.* at 1169.

[249] *Id.*

As another example, AI-based hiring assessments are the basis for recruiting-technology company HireVue, which contracts for its services with other companies.[250] HireVue's AI uses video interviews to analyze the candidate's face to determine an estimate of willingness to learn and stability.[251] Candidates that are required to interview via HireVue are not told their scores, but the scores are given to the employer.[252] The Electronic Privacy Information Center ("EPIC") filed an official complaint against the company with the Federal Trade Commission ("FTC"), arguing that the collection of biometric data is intrusive and causes substantial privacy harms.[253] The analysis is secret, which makes it impossible for the candidates to know how their personal data is being used, in turn making it impossible to consent to the use.[254] The complaint alleges that the use of AI in decision-making is dehumanizing and invasive, as it is built entirely on science that perpetuates discrimination in hiring practices.[255] The complaint asks the FTC to stop this use of automation and make the algorithms public.[256]

Using AI in college admissions and retention would lead to similar concerns. Furthermore, it highlights some of the issues that are being perpetuated by the use of big data in decision-making. Like employers, universities run the risk of creating algorithms that perpetuate biases in the datasets. Algorithms can have profound impacts on the diversity of the student population and create the risk of false positives. Because of the way the algorithms are created, it could flag students falsely for concerns such as high dropout risk. False positives not only embarrass students, but also waste university resources and undermine the efficacy used to justify big data.

D. Big Data Case Study

The aforementioned New America Foundation report includes a case study of two universities that use big data.[257] Mount Saint Mary's University, as previously mentioned, sought to use big data to identify at-risk students so they could be urged to leave the school before their data could be included in retention rate statistics reported to the federal government.[258] The other school included in the report, Georgia

[250] Drew Harwell, *Rights Group Files Federal Complaint Against AI-Hiring Firm HireVue, Citing 'Unfair and Deceptive' Practices*, WASH. POST (Nov. 6, 2019 11:50 AM), https://www.washingtonpost.com/technology/2019/11/06/prominent-rights-group-files-federal-complaint-against-ai-hiring-firm-hirevue-citing-unfair-deceptive-practices [https://perma.cc/GQF8-N39T].

[251] *Id.*

[252] *Id.*

[253] *Id.*

[254] *Id.*

[255] *Id.*

[256] *Id.*

[257] Ekowow & Palmer, *supra* note 203.

[258] *Id.*

State University, analyzed student grades over a ten-year period to determine a list of factors that indicate the likelihood of a student graduating.[259] The school then implemented a system that created alerts to show advisors which students needed help.[260] Two of these alerts are centered around the student's major; one alert occurs if the student does not sign up for a required class, and the other occurs if a student signs up for a non-required class.[261] The system has resulted in a six-year graduation rate of 52%, which is higher than the national average of 43%.[262] This case study indicates that not every university will use the results of big data in an inappropriate way and notes the great power big data gives administrators. However, the opportunities for exploitation of the data are numerous.

Admittedly, big data from surveillance does provide some benefits to higher education. However, these benefits alone are not enough to outweigh the costs of persistent surveillance of college students. Even Georgia State University's graduation rate success came at a cost to students. The school admitted that one of the system alerts happens when a student signs up for a class that is not required for that student's major. The alert will then prompt a discussion with an advisor. This discourages students from taking classes that interest them if they may be outside their chosen major. Even if a class is not within the student's major, there is value in taking classes that interest the student and expanding overall intellect. The Association of American Colleges and Universities surveyed employers and found that four out of five employers think students should have broad knowledge in liberal arts and sciences.[263] This same survey also found that employers hire students based on their communication skills and ability to solve problems rather than the student's major.[264] Furthermore, as the New America Foundation report notes, big data perpetuates any discrimination found in the dataset. These factors, on top of the privacy implications, weigh in favor of disallowing big data and pervasive surveillance in higher education.

E. Failed Attempts to Preserve Privacy at Universities

A university that may seek to implement models of privacy, such as data-as-payment or pay-for-privacy models, to combat the use of big data would still undermine student autonomy and decision-making. As Professor Stacy-Ann Elvy lays out, there are models of privacy

[259] *Id.*

[260] *Id.*

[261] *Id.*

[262] *Id.*

[263] Alexandra Vollman, *The Liberal Arts: A Broad Education for Lifelong Success*, INSIGHT INTO DIVERSITY (May 23, 2016), https://www.insightintodiversity.com/the-liberal-arts-a-broad-education-for-lifelong-success/ [https://perma.cc/868D-8JLU].

[264] *Id.*

where data is a currency.[265] The first, data-as-payment, is what social media platforms, such as Facebook, and cell phone applications use.[266] The user ostensibly gets a free service, but in exchange for that service the user is giving up data.[267] However, users may be unaware that the free service they are receiving comes at the cost of personal data.[268] Under this model, the consumer's data is a currency that is paying for the service.[269]

The pay-for-privacy models commodify privacy as something that can be bought and sold.[270] The first form of pay-for-privacy is the privacy-as-luxury model.[271] Under this model, companies provide services with more privacy if the consumer is willing to pay more for the service.[272] The model exists because there are consumers who are willing to pay for privacy, indicating privacy is on the minds of at least some consumers.[273] This means that companies can sell services for free using data-as-payment, or sell the same product for a price with built-in privacy controls, so that the consumer is not data mined.[274]

Another model is the privacy-discount model.[275] Under this model, consumers are paying for privacy, but the company offers an incentive, in the form of a discount, if consumers are willing to give up some of that privacy.[276] Companies receive revenue in the form of data from consumers who select the discount and money from consumers who are unwilling to give up their privacy.[277] When consumers engage with companies under this model, they are effectively getting paid for their data.[278]

Modeling privacy in this way creates issues instead of solving them. Models of privacy that require payment for privacy creates unequal access to privacy.[279] Under these models, only those who can afford the higher price get privacy, which creates a divide between those who get privacy and those who do not.[280] An example is research based on incomes of iPhone users versus Android users.[281] Apple's iPhone has greater security, and the company implements measures to protect

[265] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1387 (2017).
[266] *Id.* at 1385.
[267] *Id.*
[268] *Id.*
[269] *Id.*
[270] *Id.*
[271] *Id.* at 1388.
[272] *Id.*
[273] *Id.*
[274] *Id.*
[275] *Id.* at 1391.
[276] *Id.*
[277] *Id.*
[278] *Id.*
[279] *Id.* at 1400.
[280] *Id.*
[281] *Id.*

information.[282] Comparatively, Android has weaker privacy and security protections.[283] Apple's iPhone is much more expensive than its Android counterpart, with an iPhone starting at $399 compared to Android's $60.[284] The research indicates that iPhone users have higher incomes than Android users.[285] Thus, iPhone users pay more for better security and privacy.[286] The gap in privacy protections mirrors socioeconomic gaps.[287] Models like privacy-discounts force lower income consumers to make the choice between privacy and other needs.[288] Thus, if given the choice between privacy in data or extra cash in pocket for things like groceries or the utilities bill, lower income consumers are likely to opt for the discount in privacy-discount models.[289] In fact, the FCC, in the context of internet access, has acknowledged that low-income consumers are likely to be disproportionately impacted by pay-for-privacy models compared to other consumers.[290]

Yet another issue with these models of privacy is that consumer control and choice over data are illusory.[291] With many companies, the privacy policies and terms and conditions show that they can still monetize consumer data under certain conditions.[292] Often, companies do so by anonymizing the information to justify disclosure.[293] However, this relies on an assumption that consumers do not want to share data with their names attached, instead of the reality that there are many other reasons why consumers may not want to share data.[294] There is always the risk that the data can be de-anonymized and re-identified,[295] like in the aforementioned Netflix example. Additionally, the information is used to make inferences and predictions, over which the consumers have no control.[296] As a result, companies treat consumers differently based on these predictions.[297]

It is easy to see why these privacy models may appeal to universities, as they are low-cost options that may make the university money. However, the same concerns in the consumer setting presented above apply in the university setting. First, these privacy models still

[282] *Id.* at 1401.
[283] *Id.*
[284] *Id.*
[285] *Id.*
[286] *Id.*
[287] *Id.* at 1402.
[288] *Id.* at 1405.
[289] *Id.*
[290] *Id.* (citing Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87,274 (Dec. 2, 2016)).
[291] *Id.* at 1413-14.
[292] *Id.* at 1414.
[293] *Id.* at 1415.
[294] *Id.*
[295] *Id.*
[296] *Id.*
[297] *Id.*

undermine student autonomy and ability to innovate. Second, these privacy models will have a disproportionate, negative impact on low-income students, who may be receiving need-based scholarships. These students may feel as if their scholarships depend upon allowing data mining. Even in a situation where a student does not have a scholarship hanging in the balance, if giving up privacy for a discount is an option, lower income students will feel pressured to do so in order to cut back on costs of attendance. These options leave a portion of the student population feeling marginalized and left with no meaningful options. Even if universities did not care about the impact to lower income students, these types of privacy models at a university will have a negative impact on the datasets the university uses to make a predictive model. The data may be skewed, reducing the accuracy of the predictive model.

A pay-for-privacy model should be prohibited at universities. This form of "privacy" would not protect students and would instead harm them. For universities to truly protect students and create an environment in which autonomy can flourish, true privacy protections are needed on college campuses.

III. PROTECTING STUDENT PRIVACY

Universities operate under mantras that champion autonomy and innovation yet violate those principles when they data mine students. Universities could self-regulate to provide student privacy while also getting the data the university needs for student retention purposes, but they are unlikely to do so voluntarily. As a result, legislation is needed. The statutes that currently govern student privacy at universities are inadequate. Amendments to current legislation could provide greater privacy protections and could potentially be modeled after provisions of the California Consumer Privacy Act and the European Union's General Data Privacy Regulations.

A. University Self-Regulation for Student Privacy Protections

Universities use big data because they think it is the best way to gauge student success and retention, but universities are undermining students' potential to be productive and democratic citizens. Universities should want to protect student privacy, thereby protecting student development and autonomy, because it is part of the very reason that universities exist. For example, the University of Arizona's stated purpose includes expanding human potential.[298] Additionally, the university's mission statement states, "We will continuously improve how we educate and innovate so we can lead the way in developing disruptive problem-solvers capable of tackling our

[298] *Purpose and Values*, UNIVERSITY OF ARIZONA, https://www.arizona.edu/purpose-values/ [https://perma.cc/7MPM-MBB6] (last visited April 5, 2021).

greatest challenges."[299] Similarly, the University of North Carolina includes the word "liberty" as a defining principle of the university.[300] The university's mission statement also includes serving as a center for creativity.[301] These mission statements explicitly mention qualities of student development that are protected by privacy. Thus, in order to fulfill their missions, universities need to implement measures to protect student privacy and prohibit data mining of students, thus promoting autonomy.

Data mining does not further the goal of education, which is the primary purpose of universities. As mentioned above, a lack of privacy and environment of surveillance change the way students will learn. Students who drop out obviously miss out on learning. Universities should want to identify and help those students. However, in using big data to do so, universities are identifying those students by imposing costs on the entire student body. While data mining harms students' ability to learn, privacy would remedy the harm. To stay true to their purposes, universities should provide privacy to their students and seek different means to identify struggling students, allowing autonomy to flourish and students to learn.

Students could put pressure on administrations to stop the use of big data or, at a minimum, be transparent about it. Many college campuses have a powerful student government organization that helps shape decisions that impact the entire student body. If these organizations would take notice of the use of big data on campus, they could pressure the administration to change course. This sort of pressure is unlikely to occur until students are aware that data mining is occurring. This requires university transparency or some type of notice to students from advocates.

1. *Self-Regulating Through Nudge and Notice*

Universities could take steps to further privacy interests of their students, while still getting the data that they want. Universities could avail themselves of the regulatory mechanisms that legislators use to influence behavior without passing new laws.[302] "Nudging" is one mechanism used to influence behavior that exploits the ways humans tend to make irrational choices.[303] The point of nudging is that by setting the right default, it can reduce the costs of failure to switch.

[299] *Id.*

[300] *Mission and Values*, UNIVERSITY OF NORTH CAROLINA, https://www.unc.edu/about/mission/ [https://perma.cc/7BQU-SJ69] (last visited April 5, 2021).

[301] *Id.*

[302] *Ryan Calo, Code, Nudge, or Notice?*, 99 IOWA L. REV. 773, 775 (2014).

[303] *Id.*

In addition to nudging, notice is used to disclose facts to individuals in hopes that individuals will make the best choices for themselves.[304]

Nudging is effective because it uses individuals' cognitive biases in a way that helps them make productive choices.[305] The concept of nudge built upon economist Herbert Simon's work in behavioral economics, which found that people deviate from rational decision-making in predictable ways.[306] Professors Richard Thaler and Cass Sunstein strongly urge the use of nudging to leverage these irrational behaviors to get desired results.[307]

The use of defaults is the most popular version of nudging.[308] Defaults could include automatic enrollment in some form of program.[309] Defaults work because humans have a tendency to prefer the status quo and will not likely deviate from a default.[310] When a university sets a default at the preferred outcome, such as opting into data mining, it places the burden on the student to opt out.[311]

Notice is another popular form of nudging.[312] Mandated notice requires disclosure of practices to users.[313] Mandated disclosure assumes there is a gap in knowledge between the user of the product and the provider.[314] Notice serves to bridge the gap.[315] Thus, the basic premise of notice is that, with more knowledge, users will make better informed choices.[316] When imposed as a regulation, which is often the case in privacy, the regulated entity must provide notice at a decision point.[317] Notice can come in the form of lengthy reports targeting sophisticated parties or communications like a letter or email.[318] Given how versatile notice can be, it is the regulation of choice for legislators, as it requires little cost for regulated entities and does not require legislators to tell the entity how to run its business.[319] Further, notice places the burden on consumers to choose from among competing options, so long as they have knowledge of those options.[320] Thus, mandating notice is a win all around for legislators.

[304] *Id.*

[305] *Id.* at 783.

[306] *Id.*

[307] *See* Richard H. Thaler & Cass R. Sunstein, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

[308] Calo, *supra* note 302, at 785.

[309] Cass R. Sunstein, *Nudging: A Very Short Guide*, 37 J. CONSUMER POL'Y 583, at 3-4 (2014).

[310] Calo, *supra* note 302, at 785.

[311] *Id.*

[312] *Id.* at 787.

[313] *Id.*

[314] *Id.*

[315] *Id.*

[316] *Id.*

[317] *Id.*

[318] *Id.* at 788.

[319] *Id.*

[320] *Id.*

Universities could utilize nudging to push students towards sharing data for retention purposes. Universities can set the default at data mining while providing notice of why the data is needed to further student retention goals. Further, universities could give students the opportunity to opt out. Since student retention after the first year is so important, universities can set the default and place the notice at the outset of the relationship between the students and the university. If universities truly need the student data for retention purposes, this would allow the universities to still get the data needed, while providing better privacy protections for the students.

Nudging is a good default for a large number of people, but a better default would be to start with disclosure to the students. As part of the disclosure, the university could provide a nudge, fully explaining the purpose of the data mining and benefits of it. Students then would have the choice to opt into data mining, instead of opting out. As part of this process, the university could nudge by explaining how many other schools utilize this, how many other students have agreed to allow it, and explain that it may make the first year of college easier for the students. Throughout the semester, the university could remind a student that there is still the option to opt in.

A university should utilize a combination of both nudge and notice to protect student autonomy. As mentioned above, the New America Foundation report highlights that a challenge of big data in colleges is a lack of transparency. Transparency could improve with disclosure. Disclosure should include informing students of the type of information that can be gathered about the students, such as ID card swipes and Wi-Fi activity, along with the uses of the information. The information should be disclosed at the outset of the relationship between the student and college. Further, nudging can be utilized by giving students the opportunity to opt out of data gathering without ramifications. Colleges should keep the disclosure simple so that it is easily understood.

In fact, the combination of nudge and notice has been successful. Virginia Commonwealth University provides an example of effective disclosure. In the fall of 2019, the university tested a new program that compared students' Wi-Fi connection with the students' class schedules to determine if the students attended class.[321] Disclosure was provided in the form of answering frequently asked questions.[322] The university explained how the information was gathered, why the information was gathered, and which classes were participating in the test program.[323] Along with the information about the program, the

[321] *Student Success*, VIRGINIA COMMONWEALTH UNIVERSITY, https://studentsuccess.vcu.edu/ramattend/archive [https://perma.cc/6CRG-EZQK] (last visited Sept. 19, 2020).

[322] *Id.*

[323] *Id.* Notably, student retention and graduation are the cited reasons for the program.

university provided a link through which students could opt out of the program by late November 2019. As of January 2020, there were 4,047 students enrolled in classes that would be part of the test program. Of those students, 2,414 students opted out of the program.[324] This means almost 60% of students opted out of having their Wi-Fi connectivity analyzed, leaving only 1,633 students that agreed to have their data analyzed.[325] Thus, an easy-to-read disclosure can fulfill its purpose.

2. Questionable Effectiveness of Notice

However, mandated notice is not always effective and has its critics. Professors Omri Ben-Shahar and Carl Schneider criticize mandated disclosure at length.[326] One identified problem of mandated disclosure is the "more-is-better" mantra, which in turn leads to disclosure that is far too broad.[327] Legislators have a hard time discerning which data will be important to consumers, which leads to the belief that everything is useful so everything must be disclosed.[328] The result is that mandated disclosures multiply.[329]

Further, as new information comes to light, there is "constant pressure to cover newly noticed contingencies."[330] Therefore, the scope of the mandate is continually increasing.[331] As proof, Ben-Shahar and Schneider cite to a study of healthcare patients, which indicates that 76% of patients want to know about any adverse effects of treatment, regardless of how rare that effect may be.[332] Mandated disclosure also expands as a result of disclosees' incorrect interpretation of the data they are given.[333] For example, patients who were informed about doctors' and researchers' conflicts of interests thought that such a disclosure was a positive sign that the study would be done correctly.[334] As a result, more information is given to consumers to ensure they interpret the disclosure correctly, leading to overcorrection.[335] Disclosures become too copious and complex, and the disclosee cannot effectively handle the quantity of information given to them.[336]

[324] *Id.*

[325] *Id.*

[326] Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647 (2011).

[327] *Id.* at 684.

[328] *Id.*

[329] *Id.*

[330] *Id.* at 685.

[331] *Id.*

[332] *Id.* at 684 (citing Dewey K. Ziegler et al., *How Much Information About Adverse Effects of Medication Do Patients Want From Physicians?*, 161 ARCHIVES INTERNAL MED. 706, 708 (2001)).

[333] *Id.* at 686.

[334] *Id.*

[335] *Id.*

[336] *Id.* at 687.

Another problem occurs when the disclosee is given too many disclosures and cannot read and comprehend all of them.[337] These problems have no good solution.[338] A choice between incomplete disclosure or too much disclosure is no choice at all.[339] Further, when deciding to implement disclosures, legislators deal with the issues individually, while consumers deal with the disclosures all at once, each competing for the consumers' time.[340] Thus, while the length of disclosures grow, the amount of time disclosees have to read the disclosures shrinks because consumers are accosted with more and more.

Yet another issue with disclosure is articulating the information adequately.[341] Disclosures can be vague or provide precise information.[342] Providing specific information can be challenging unless all information needed for such disclosure is well known at the time of writing the disclosure.[343] For example, writing a disclosure for cigarettes was more easily done once all the dangers of smoking were widely known.[344] Conversely, providing vague disclosure does not give adequate guidance to consumers.[345] How to disclose is a related issue.[346] The decision of where to place disclosure, such as at the beginning or end of the document, raises concerns about whether it is adequately signaling the importance of the disclosure.[347]

An issue at the heart of mandated disclosure is the ability of consumers to understand the information given to them.[348] First, disclosures are hard to read.[349] For example, financial privacy disclosures require an advanced college reading level to understand.[350] Another example is HIPAA authorization, which uses language comparable to legal contracts or professional medical literature.[351] The demand for simpler disclosure has led to the realization that only modest progress is possible.[352] Consumers place the information they receive within the framework of their personal understanding, which means that it is often misunderstood because they lack requisite background information necessary for proper interpretation.[353]

[337] *Id.*
[338] *Id.* at 688.
[339] *Id.*
[340] *Id.*
[341] *Id.* at 690.
[342] *Id.* at 690-91.
[343] *Id.*
[344] *Id.*
[345] *Id.*
[346] *Id.*
[347] *Id.*
[348] *Id.* at 711.
[349] *Id.* at 712.
[350] *Id.*
[351] *Id.*
[352] *Id.*
[353] *Id.* at 717.

Additionally, a primary assumption of mandated disclosure is that consumers want to make the decisions put in front of them.[354] However, when faced with complicated decisions, consumers look for shortcuts.[355] Consumers want to use less information in order to break the information down into understandable pieces and make familiar decisions.[356] These preferences are all ignored when mandated disclosure is utilized.[357] Such disclosures may present choices that consumers do not want to make and, as a result, consumers become overwhelmed and simply do not make the choice.

B. Current Regulatory Regime

Currently, student data mining is working for universities and, as a result, it is highly unlikely that universities will change their practices on their own. The self-regulation discussed above is unlikely to happen, as universities currently see no reason not to data mine students. Thus, legislation is needed to ensure student autonomy and privacy are protected at universities. Without it, universities are unlikely to disclose student data mining or seek consent to do so. The current regulatory regime, outlined below, is inadequate to deal with the use of big data by universities.

Currently, universities are subject to the privacy protections in the Family Educational Rights and Privacy Act ("FERPA"). In 1974, FERPA was introduced by Senator James Buckley as a means of remedying privacy violations by schools that were releasing personal data.[358] Additionally, Senator Buckley wanted to give parents notice and control over disclosure of information to outside parties.[359] This desire was born out of a report published by the Russell Sage Foundation, which conducted a study that found schools did not give sufficient notice or opportunity to consent to data collection for student records.[360] The report highlighted that schools were collecting information about more than just attendance and grades.[361] Students were surveyed about their "families, beliefs, values, drug use, and sexual mores to gain insight."[362] Colleges and universities collected information about student activists to share with law enforcement.[363] Indeed, the Watergate Scandal was on legislators' minds when adopting FERPA, as they were afraid that secret files were

[354] *Id.* at 727.
[355] *Id.* at 721.
[356] *Id.* at 729.
[357] *Id.*
[358] 121 CONG. REC. 39,991 (1974).
[359] 120 CONG. REC. 39,864 (1974).
[360] Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPS*, 8 DREXEL L. REV. 339, 354 (2016).
[361] *Id.*
[362] *Id.*
[363] *Id.*

being created to make a record that would limit students' future opportunities.[364]

Today, FERPA grants parents of children under eighteen years of age and students over the age of eighteen enrolled in post-secondary institutions specific rights regarding personally identifiable information ("PII") within the students' records.[365] They have the right to inspect and review the accuracy of the record; the right to challenge the accuracy of the record at a hearing and provide correction or commentary; and the right to prevent PII collected and maintained from being disclosed to any third party without written consent.[366] PII is defined to include, but is not limited to: the student's name; the name of the student's parents or other family members; the address of the student or student's family; a personal identifier, such as the student's social security number or biometric record; indirect identifiers such as date of birth, place of birth, or mother's maiden name; other information that is linked or linkable to a specific student that would allow that student to be identified with reasonable certainty; or information requested by a person who the institution reasonably believes knows the identity of the student.[367]

However, there are exceptions when student information may be provided without student or parent consent. One exception allows disclosure of information to other school officials who are determined to have a legitimate educational interest in the records.[368] This exception also applies to a contractor to whom the institution has outsourced services or functions, so long as the contractor performs an institutional service, is under the direct control of the institution with respect to use and maintenance of education records, and is subject to the requirement that the PII be kept private.[369] Additional exceptions include processing financial aid,[370] disseminating to accrediting organizations to carry out functions,[371] assisting with a health or safety emergency,[372] and complying with a judicial order or subpoena.[373]

Universities must comply with FERPA in order to receive federal funding.[374] Colleges are required to allow the opportunity for a hearing to challenge the content of the education records to ensure that they are not "inaccurate, misleading, or otherwise in violation of the privacy rights of students."[375] If information is found to be incorrect, the school

[364] *Id.* at 355.
[365] 20 U.S.C. § 1232g(a)-(b) (2018).
[366] *Id.*
[367] 34 C.F.R. § 99.3 (2018).
[368] 20 U.S.C. § 1232g(b)(1)(B) (2018).
[369] 34 C.F.R. § 99.31(a)(1)(i)(A)-(B) (2018).
[370] 20 U.S.C. § 1232g(b)(1)(D) (2018).
[371] *Id.* § 1232g(b)(1)(G).
[372] 34 C.F.R. § 99.31(a)(10) (2018).
[373] *Id.* § 99.31(a)(9)(i).
[374] 20 U.S.C. § 1232g(a)-(b) (2018).
[375] *Id.* § 1232g(a)(2).

must allow for correction or deletion.[376] If a college is found to be in violation of FERPA, the Department of Education has the power to withdraw all public funding[377] Additionally, if a third party that the college contracts with is found to be in violation of FERPA, the school from which the PII originated may not allow access to PII by that third party for at least five years.[378] It is worth noting that, by statute, FERPA compliance is only required by schools that receive public funding.[379] Additionally, FERPA does not grant a private right of action for violations.[380] Thus, it is within the sole discretion of the Department of Education to enforce any violations.

There are a few procedural safeguards built into FERPA that grant students limited rights of enforcement of FERPA's protections.[381] FERPA designates power to the Office of the Chief Privacy Officer of the Department of Education to investigate and review complaints of violations.[382] Additionally, the Office of Administrative Law Judges ("Office") is enabled to act as a review board.[383] A student has the authority to file a written complaint alleging a violation to the Office.[384] However, this is a time-limited power, so the complaint must be filed within 180 days of the alleged violation.[385]

Once the student has filed a written complaint, the Office has the choice to complete an investigation to determine the veracity of the complaint and whether there is an actual FERPA violation.[386] If the Office decides to investigate, the complainant and school will be given written notice, which includes the allegations.[387] The notice will also instruct the school to submit a written response, which must include information about the school's policies on educational records.[388] The Office will also notify the complainant if it decides not to pursue investigation.[389] Should the Office determine that a failure to comply with FERPA has occurred, the Office may also determine whether the failure was due to a policy or practice, which will impact the steps the university must take to become compliant.[390] Additionally, the Office may ask the parties to submit written or oral arguments if needed.[391]

[376] *Id.*
[377] *Id.* § 1232g(b)(1)-(2).
[378] 34 C.F.R. § 99.67(c) (2012).
[379] 20 U.S.C. § 1232g(a)(3) (2018).
[380] Gonzaga Univ. v. Doe, 536 U.S. 273, 273 (2002).
[381] *See* 34 C.F.R. § 99, Sub. E. (2012).
[382] *Id.* § 99.60.
[383] *Id.*
[384] *Id.* § 99.63.
[385] *Id.* § 99.64(c).
[386] *Id.* § 99.64(b).
[387] *Id.* § 99.65(a)(1).
[388] *Id.* § 99.65(a)(2).
[389] *Id.* § 99.65(b).
[390] *Id.* § 99.64(b).
[391] *Id.* § 99.66(a).

At the conclusion of the investigation, the Office submits written notice of its findings and the basis for the findings to the complainant and applicable parties.[392] Should the Office find that the school has not complied with FERPA, the school will then be given a list of specific steps to take to become compliant, along with a "reasonable" timetable for when the school must come into compliance.[393] If the university does not comply with the provided steps, the Secretary of Education is authorized to take legal actions to enforce compliance.[394] This includes withholding further payments under any applicable programs, issuing a complaint to compel compliance through a cease-and-desist order, or terminating eligibility to receive funding under any applicable program.[395]

While this process places some power in the hands of students, it does not correct the individual harms suffered by the student who files the complaint. At most, this power ensures that a situation similar to that in the complaint does not occur again but does not allow remedy for the student individually. The harmed students are left with no remedy for the violations because there is no private right of action. Additionally, filing a complaint in no way guarantees that the Office will investigate. Filing a complaint effectively does nothing more than alert the Office to the fact that there may be a FERPA violation; it still leaves all discretion in the hands of the Office and out of the hands of the students.

The exception to consensual disclosure for school officials is troubling. The school official exception grants schools the authority to determine who is a school official and what are legitimate educational interests.[396] Additionally, the determination under the exception is informal.[397] No formal designation is required nor is specification of the purpose behind the disclosure or even any data security mechanisms.[398] There are also minimal oversight requirements under FERPA governing the third-party outsourcing of schools' official duties.[399] All that is required is that colleges use "reasonable methods" to exercise "direct control" to ensure compliance.[400]

There is also no requirement that the relationship between a college and third-party provider be governed by a contract.[401] While a contract may not solve all problems, the lack of a contract requirement means that there is not even a bare minimum standard that must be

[392] *Id.* § 99.66(b).

[393] *Id.* § 99.66(c).

[394] *Id.* § 99.67(a).

[395] *Id.*

[396] Zeide, *supra* note 360, at 359-60.

[397] *Id.* at 360.

[398] *Id.* at 361.

[399] *Id.*

[400] 34 C.F.R. § 99.31(a)(1)(ii) (2018).

[401] Zeide, *supra* note 360, at 362.

met. Furthermore, the Department of Education has not defined "reasonable methods" or "direct control."[402] At most, the Department of Education has only referenced best practices in a non-binding document.[403] In the non-binding guide, the Department of Education has only suggested that reasonableness corresponds with the level of harm presented by the information while also reflecting practices at similarly situated schools.[404] Lastly, the Department of Education defers to the institution's determination of a legitimate educational interest.[405]

The protections offered by FERPA rely on the presumption that disclosure of information occurs pursuant to oversight and approval.[406] It also assumes that educational decision makers use the student data wisely.[407] These presumptions no longer hold true in the age of big data and the prevalent use of outside parties to provide services based on data.[408] The limiting safeguards of FERPA do not account for the wealth of information that can be derived from student data.[409] FERPA is not prepared to address the privacy concerns that arise from universities' use of student ID card swipes to determine social interactions and networks or system alerts to identify at-risk students.

C. Fixing FERPA

There are three ways FERPA could be fixed. First, FERPA could be amended to provide better protection in light of big data. Next, FERPA could be interpreted differently, allowing PII to cover the student data currently being gathered. Finally, litigating FERPA violations will provide little help in fixing the statute.

1. Amending FERPA

Amendments to FERPA have been proposed that increase transparency and notice in an attempt to give students and parents more control.[410] These proposed amendments have focused on constraints on collection, use, retention, and repurposing of data.[411] Further, the proposed amendments have attempted to add regulations so that third parties must meet a higher threshold to qualify to receive

[402] *Id.*

[403] *Id.*; *see also* U.S. DEP'T OF EDUC. PRIVACY TECH. ASSISTANCE CTR., Guidance for Reasonable Methods and Written Agreement (2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Guidance_for_Reasonable_Methods%20final_0.pdf [https://perma.cc/A7WT-9538].

[404] Zeide, *supra* note 360, at 362.

[405] *Id.* at 365.

[406] *Id.* at 373.

[407] *Id.*

[408] *Id.*

[409] *Id.*

[410] *Id.* at 379.

[411] *Id.* at 379-80.

the data.[412] Some of these proposed amendments would require private contracts that include explicit penalties for breaches of the agreement.[413] However, these proposed amendments have remained just that: proposals that are not law.

Any proposed amendment to FERPA should strengthen privacy protections compared to those already provided by the statute. Strengthening the privacy protections would promote student autonomy and choice. The language of FERPA and subsequent interpretation does little to address the sort of data being gathered by colleges today. It is unclear whether data such as ID card swipes with time stamps and location information or Wi-Fi connection activity is the type of data regulated by FERPA. It is likely not. Currently, FERPA only protects students' personally identifiable information. The current definition of personally identifiable information does not explicitly include data from ID card swipes and Wi-Fi connectivity. That data is gathered and used in a way that is not as easily linked to the student in ways that FERPA contemplates. As a result, these forms of data are not defined as personally identifiable information.

Even if the information were classified as personally identifiable information, students have no ability to protect it, aside from the ability to review the record. Additionally, ID card swipes and Wi-Fi connectivity are not part of an educational record of the sort that FERPA was designed to protect. FERPA defines an educational record as materials that have information directly related to a student that are maintained by the school.[414] Instead, the ID card swipes and Wi-Fi connectivity are used to feed into the algorithm monitoring students. If FERPA is to address these problems, proposed amendments must address this sort of data collection to ensure universities are not creating an environment of constant surveillance. Amendments to this effect would align with the initial reasoning behind enacting FERPA in the 1970s. Today, more so than decades ago, colleges have the capability of learning intimate detail of students' lives to create "secret files" on students.

2. Interpreting FERPA

Alternatively, as opposed to amending FERPA, the Department of Education could institute rulemaking to address the issue of student privacy. Using its rulemaking authority, the Department of Education could promulgate guidance for institutions of higher education to prohibit data mining of students. Notably, the Department of Education is required to use negotiated rulemaking, involving interest groups in the rulemaking process.[415] Currently, the Department of

[412] *Id.* at 380.

[413] *Id.*

[414] 20 U.S.C. § 1232g(a)(4)(A)(i)-(ii) (2018).

[415] *See id.* § 6571.

Education has rules that supplement FERPA, providing definitions and filling in the gaps of the statute.[416] Without amending FERPA, the Department of Education could provide more rules within this section to provide greater student protection.

One such rule could be to expand the definition of personally identifiable information. This rule could expand the definition to include the type of data currently being gathered by universities, such as ID card swipes and Wi-Fi connectivity. Further, the definition of educational records could be expanded to include the records generated by universities as they use big data to analyze student behaviors. The rule should also define what exactly constitutes a legitimate educational interest. Big data analysis would not be a legitimate educational interest. Additionally, a rule could be added to govern the relationships between universities and third-party vendors of data processing. The rule could create parameters to govern the relationship between universities and third-party vendors.

3. Litigating FERPA

Absent legislative help, courts will not be very useful in filling the gaps in FERPA. There is a dearth of case law providing guidance on the current holes in FERPA's definitions. This is largely because there is no private right of action under FERPA for students or parents to bring suit. However, an individual may challenge a Department of Education rule if the individual can show that they suffered a concrete and particularized harm.[417] The statute also explicitly directs the Secretary of Education to limit funds.[418] Thus, courts have little, if any, opportunity to rule on FERPA language and help fill any holes. This leaves interpretation of questionable language to the sole discretion of universities, with little oversight and ability to correct if the school officials are incorrect in their interpretation. The Secretary of the Department of Education does, however, designate the Office of Administrative Law Judges to act as a review board for programs that fall under FERPA's domain.[419] This is the main form of review available under FERPA, and the purpose of this review board is solely to act as part of the Department of Education to investigate violations or complaints.[420] The review board would only be able to investigate big data usage if it is alleged by the complainant, which in turn requires the complainant to know data is being used.

[416] *See* 34 C.F.R. Sub. A, Pt. 99.

[417] *See* Elec. Privacy Info. Ctr. v. U.S. Dep't of Educ., 48 F. Supp. 3d 1, 14-15 (D.C. Cir. 2014).

[418] *See* 20 U.S.C. § 1232g(b)(1) (2018).

[419] 34 C.F.R. § 99.60(c) (2018).

[420] *Id.* § 1232g(g).

D. Proposed New Legislation

Instead of amending FERPA, Congress might instead enact federal privacy protection similar to the California Consumer Privacy Act ("Act" or "CCPA"). Enacted in 2018, the CCPA provides consumers in California with many more rights than federal privacy statutes. Under the Act, consumers have the right to request that businesses which collect consumers personal information disclose what has been gathered.[421] This includes what type of personal information has been gathered, the sources from which the personal information is collected, the business purpose behind collection, the third parties with whom the business shares the information, and the specific pieces of personal information the business has collected about the consumer.[422] Additionally, businesses that want to collect a consumer's personal information must inform the consumer either at the time of collection or before collection regarding what type of information will be collected and why.[423]

Consumers may also request that businesses delete data, and businesses must inform consumers that they have the right to request deletion.[424] If requested, the business must delete the information and direct any third-party service providers to do the same.[425] Importantly, businesses may not retaliate against a consumer who exercises these rights by denying goods or services, providing a different quality of service, charging a different price for the good or service, or even suggesting retaliation.[426] Businesses must also provide consumers with the right to opt out of collection.[427] Importantly, businesses cannot attempt to get around the Act contractually.[428] The Act also provides a right of action to a consumer whose information is subject to an unauthorized access, theft, or disclosure because a business failed to follow its duty to implement security procedures.[429]

While the Act is limited to businesses,[430] the structure readily lends itself to the context of colleges' information collection from students. It is easy to see how the information collected by colleges, such as ID card swipes and Wi-Fi connectivity, could be regulated by statutes like the CCPA.

Unfortunately, colleges in California are only saved from the Act if they are classified as not-for-profit.[431] Any for-profit college operating

[421] CAL. CIV. CODE § 1798.100(a) (West 2018). .

[422] *Id.* § 1798.110.

[423] *Id.* § 1798.100(b).

[424] *Id.* § 1798.105(a)-(b).

[425] *Id.* § 1798.105(c).

[426] *Id.* § 1798.125(a)(1)(A)-(D).

[427] *Id.* § 1798.135.

[428] *Id.* § 1798.192.

[429] *Id.* § 1798.150.

[430] *Id.* § 1798.140.

[431] *Id.* § 1798.140(c)(1).

in California that has an annual gross revenue over $25,000,000 that buys, receives, sells, or shares personal information of more than 50,000 individuals, or gets 50% or more of annual revenues from selling information could be subject to the Act.[432] Likely this is an unintended consequence, but the for-profit and not-for-profit distinction essentially leaves a loophole that allows state and federally funded colleges to get away with data mining that their for-profit counterparts could not.

Instead of amending FERPA, Congress should implement a federal version of the California Consumer Protection Act that focuses on student privacy. The easiest way to do this would be to simply alter the Act's definitions to apply to all colleges that are data mining students and tailor the Act's regulations to colleges. To promote transparency, students should be able to find out what information their college has collected about them, who it is being shared with, and for what purpose. In a sense, college students are no different than any other consumer; the good that is being consumed is just slightly different than what is traditionally thought of as a good or service. Nevertheless, making the choice of which university to attend is no different than a choice between other goods and services, based on price and other features that are important to the consumer. A federal version of the CCPA would put students' data back into the students' hands and allow the students to make the ultimate decision about their personal information, instead of leaving it up to the Department of Education to remedy violations. Additionally, students would finally have a right of action for violations that students have never previously had. Students would not have to fear repercussions for their personal decisions regarding usage of personal information, such as an increase in tuition or loss of scholarship that may otherwise lead them to accept data mining.

However, any federal version of CCPA is far from fruition. Legislators may not be keen to pass something quite this bold. With election always on their minds, it is unlikely legislators would pass something that businesses within their constituency might disfavor. Additionally, legislators would not want to allow a cause of action for privacy violations, as litigation may be seen as a waste of time or resources for colleges. Thus, the definition of PII could be expanded to include information like ID cards, which can actually be tied to a student's personal information through name and date of birth. Currently, the definition includes "other information that . . . is linked or linkable to a specific student that would allow [that student to be identified] with reasonable certainty."[433] ID card use and Wi-Fi connectivity are easily linked to individual students, hence why universities want to use them to identify whether a student is in class

[432] *Id.* § 1798.140(c)(1)(A)-(C).

[433] 34 C.F.R. § 99.3.

or other places on campus. Once linked to a student, it is linked to the other PII that the school has in its records. Thus, an expansion of the definition to include these forms of information would be a step in the right direction.

Alternatively, instead of applying more regulations on colleges, legislators might consider legislation that regulates the third-party vendors that are contracting with the colleges. These regulations could ensure that these companies do not receive students' personally identifiable information and, instead, only get aggregate student data that cannot be tied to any one student. Further, any regulation of the vendors should ensure that the companies are unable to sell student data to any other parties for any purpose. Regulations should place time limits on data retention and address how companies should respond in the event of a data breach. Lastly, the regulations should provide students with a cause of action for violations. A cause of action would allow companies to be held accountable for mishandling students' data and also allow students a remedy for misuse.

E. Comparison to European Data Privacy Protections

Current federal privacy protections look particularly thin in light of the European Union's General Data Protection Regulations ("GDPR"). The GDPR grew out of the 1995 Data Protection Directive ("Directive"), which at the time provided unprecedented personal data protections.[434] By replacing the Directive with the GDPR, the EU kept pace with technological advances.[435] Specifically, the GDPR gives consumers control of their information collected by businesses.[436] The regulations apply not only to businesses within the EU, but also to businesses outside the EU if the business offers goods or services to EU data subjects.[437] The GDPR recognizes two types of data handlers.[438] The first is a controller, which is defined as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[439] The other is a processor, which is the person or other body that processes personal data on behalf of the controller.[440] Under the GDPR, data privacy is a fundamental right.[441] This belief is reflected in the main principles of the GDPR:

[434] Beata A. Safari, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*, 47 SETON HALL L. REV. 809, 811-12 (2017).

[435] *Id.*

[436] *GDPR FAQs: Frequently Asked Questions About GDPR*, EU GDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs/ [https://perma.cc/3WBX-EEE4] (last visited Feb. 12, 2019).

[437] *Id.*

[438] General Data Protection Regulation 2016/679, art. 4, 2016 O.J. (L 119) 33.

[439] *Id.* art. 4(7).

[440] *Id.* art 4(8).

[441] *Id.* Recital 1, at 1.

(1) "lawfulness, fairness and transparency;" (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; and (6) accountability.[442] The GDPR also contains a set of criteria that must be met for lawful data processing, such as getting consent from the data subject.[443] After the information has been gathered about the data subject, the GDPR also grants rights to the data subject to access the data.[444] Another feature of the GDPR is the responsibilities of the controller to implement safeguards into the data processing.[445]

The nuances of the GDPR sets limits that colleges within the United States would need to comply with if providing any goods or services within the European Union. First, colleges would need to meet the criteria for lawful data processing. Obtaining consent from the data subject is the first criterion.[446] Under the GDPR, consent is crucial. The data controller, here the university, has the burden of proving that the data subject gave consent.[447] Further, consent must be requested from the data subject in clear and plain language.[448] If consent appears to have been required as a necessary condition for performance of a contract, that weighs in favor for finding consent was not freely given.[449] Most colleges do not meet this consent requirement, as students may be unaware that data collection is even happening. Further, even if students knew collection was occurring, their consent must be clearly and unambiguously given. However, even in situations where the university has obtained consent, it may be challenging for the university to prove that the student did not believe consent was required to attend the school or take a particular class; it is easy to see how students may believe attendance is conditioned on consent.

Next, under the GDPR, lawful data processing requires compliance with the data controller's legal obligations, that the data controller protect the data subject's vital interests, that there is a need to process the data is for a public interest, and that there are legitimate interests in the data that do not override the data subject's fundamental rights.[450] Student data collection is hardly part of the school's legal obligations, nor is it necessary to carry out some sort of public interest; although universities may argue that improving student retention is a public interest. Further, as argued above, the environment of surveillance created by this data gathering at universities goes against the interests of students, rather than protecting them.[451] Finally,

[442] *Id.* art 5(1)(a)-(f).
[443] *Id.* art. 6(1).
[444] *Id.* art. 15.
[445] *Id.* art. 25(1).
[446] *Id.* art. 6(1)(a).
[447] *Id.* art. 7(1).
[448] *Id.* art. 7(2).
[449] *Id.* art. 7(4).
[450] *Id.* art. 6(a)(c)-(f)
[451] *See supra* notes 59-262 and accompanying text.

under the GDPR, data privacy is a fundamental right. Therefore, data mining of this sort may be overridden by the data subject's fundamental rights, even if the university argues that student retention is a public interest.

The GDPR also places responsibilities on the controller of the data. These responsibilities would apply not only to the colleges, but also to third-party vendors that analyze the data.[452] Colleges and third-party vendors would need to keep detailed records of data processing.[453] The records must include security measures and time limits for erasure.[454] Further, the colleges and third-party vendors would be required under the GDPR to have a binding contract, which would specify what data was to be processed.[455]

Yet another burden placed on both parties would be to ensure that there are safeguards in place so that the only data processed is for the exact purpose for which it is gathered.[456] This means that if a university decides to monitor students' Wi-Fi connectivity to determine if the students were in class, that is the only purpose for which the Wi-Fi connectivity data can be used. The data could not be used to determine if the student had a routine, such as going to the on-campus gym or library after class, in order to figure out how likely the student is to return after freshman year. If consent were given to track data for one purpose but instead used for another, the university would not have consent for that usage. Again, this would apply not only to the colleges but also to the third-party vendors in possession of the data. Thus, the purpose of the data gathering would have to be determined and communicated at the outset and strictly followed to ensure compliance with the GDPR.[457]

Aside from additional requirements the colleges and third-party vendors would have to follow, students would have more rights with regards to the gathered data under the GDPR. Under the GDPR, students would have a right of access to the data.[458] This means that students would be free to request and obtain access to any information that the college may have gathered about the student.[459] The right would include not only what has been gathered, but how and why it was gathered. Additionally, the student could learn who is going to receive the data and how long the school or third party will store the data. Finally, the student would be on notice that they have a right to have the information erased or lodge a complaint.[460]

[452] General Data Protection Regulation 2016/679, art. 28, 2016 O.J. (L 119) 33.

[453] *Id.* art. 30(1).

[454] *Id.*

[455] *Id.* art. 28(3).

[456] *Id.*

[457] *Id.* art. 12.

[458] *Id.* art. 15

[459] *Id.* art. 15(1).

[460] *Id.*

Specifically, the "right to be forgotten" is an important right that is unlike any right a student has under American law. It means that after the student leaves the university, the student would be able to request that all information gathered on them be completely deleted by the school and any applicable third parties.[461] Students would also be free to fix any inaccurate or incomplete information[462] or to restrict any further processing of their data.[463] These rights put control into the hands of students rather than the universities. It also grants an effective right of oversight to students, enabling them to be sure that the university is living up to promises that it made. The right of access also allows students to hold third parties accountable if the university fails to do so.

A final right is the right to be free from automated decision-making.[464] The right is essentially the right to be free from profiling that uses data analytics and algorithms. If the data controller wished to use automated decision-making, there would need to be some level of human intervention.[465] If the right were recognized in the United States, universities' current practices would regularly violate it. The data is used to generate algorithms that in turn can be used to predict behavior. This function is in direct violation of this major tenant of the GDPR. Thus, universities would be unable to engage in surveilling students like this in the European Union. The right strips away the underlying incentive behind data mining. Without the ability to create the predictive algorithms, there is less incentive for universities to data mine.

Notably, the scope of the GDPR raises the question of whether American universities might also be in violation of the GDPR. As mentioned above, the GDPR is applicable to businesses outside the EU that offer services to EU data subjects. It is unclear whether this would also apply to American colleges with students who are EU citizens studying in the United States. If so, then any college engaging in data mining and profiling of these students could be found in violation of the GDPR.

A comparison of FERPA, the California Consumer Privacy Act, and the GDPR highlights how comparatively little protection is afforded to students under FERPA. Regimes like the CCPA and GDPR place rights in the hands of the data subjects. One key feature of the GDPR that should be transplanted into legislation in the United States as a right for American students is the right to be free from automated decision-making or profiling. Under the GDPR, this feature is the most detrimental to big data and the use of algorithms to make decisions. A

[461] *Id.* art. 17.

[462] *Id.* art. 16.

[463] *Id.* art. 18.

[464] *Id.* art. 22

[465] *Id.*

well-rounded student privacy regime would incorporate all the important aspects of the CCPA and GDPR. Privacy protections like these would promote the true goal of higher education, which is learning. Students would be free to learn autonomously and have space for innovation. Further, choices about a student's future and career would not rely on algorithms that indicate a red flag when an inquisitive student signs up for a class that is not required for that student's major. Students would learn and grow into better citizens, equipped to play meaningful roles in democracy.

CONCLUSION

This Note has highlighted the problems big data can cause to student development at the university level. Further, the use of big data undercuts the purpose behind a university: to create an environment where students can learn. Therefore, by changing the university environment from one in which autonomy can flourish to one of surveillance, universities are changing the way students learn and negatively impacting their ability to be self-governed, democratic citizens. Furthermore, universities should take note of the issues that are popping up with the use of big data and artificial intelligence in the realm of employment hiring decisions. Ultimately, universities may be perpetuating biases and harming protected classes. As a result, true privacy, not a version where students must pay for it, should be provided by universities. Current privacy regulations are not strong enough to protect students. Thus, Congress should step in and implement change to effectively protect students. However, given the unlikelihood of that happening, society and students must pressure universities to do better. Consequently, disclosure is necessary, along with a choice to allow students to opt out of data mining. Additionally, a lack of transparency is a persisting problem regarding universities' usage of big data. In an effort to be transparent, universities could utilize disclosure and a variety of nudging techniques, while still getting data and simultaneously providing some protections for students who desire it. Without top-down privacy regulations, an outright stop of these practices will likely not occur. However, bottom-up regulation can have the same impact, as the story of Virginia Commonwealth University demonstrates. The time has come for universities to start being transparent about their use of big data and provide students some measure of control.