HIGHER EDUCATION VOICES:

College Students' Attitudes Toward Data Privacy

BY JASMINE PARK AND AMELIA VANCE[1]

FUTURE OF PRIVACY FORUM

EXECUTIVE SUMMARY

A popular belief is that people who have grown up using digital technologies have little concern for the privacy of their data. This belief is particularly concerning because many in this age group live much of their academic and personal lives online, and some data holders have used this belief to justify inadequate privacy practices. Moreover, even before the COVID-19 pandemic forced many colleges and universities to transition to online learning, higher education institutions had increasingly depended on online platforms for student learning, advising, and management, in order to optimize processes and deliver student services at scale.

Today's students will become tomorrow's software engineers, technology entrepreneurs, and professionals in other fields integral to the digital realm. Their attitudes toward data privacy will shape the policies and practices that govern the internet. As such, society needs to better understand college student attitudes, expectations, and behaviors regarding data privacy, and take a more active role in shaping behaviors.

To help meet this need, the Future of Privacy Forum (FPF) reviewed publicly available qualitative and quantitative research studies on the data privacy preferences, attitudes, and behaviors of college and university students in the United States and other countries. The results revealed that college students care deeply about data privacy, and their concern appears to be increasing. These students prioritize protecting information related to their academic and professional prospects but also care about safeguarding their personal information. They want universities to use their personal information predominantly for educational purposes. They want protection for immutable identifiers, such as biometric information, in higher education contexts. They also have greater confidence in education institutions and government than in technology companies.

Considering these results, FPF offers the following recommendations for research and practice:

- Higher education institutions should teach data privacy, ethics, and digital literacy courses to encourage college students to think critically about data privacy.
- To foster trust and cooperation, higher education institutions and technology companies should communicate how and why they collect, use, and share students' personal information.
- Researchers should conduct further studies on college students' attitudes, expectations, and behaviors regarding data privacy.

INTRODUCTION

The current generation of college students often bears the moniker *digital natives*, referring to individuals immersed in digital technologies from a young age and who see these technologies mediating nearly all aspects of their lives. College-age young adults in the US conduct much of their personal and academic lives online. A 2018 Pew Research Center survey found that almost all Americans aged 18 to 24 use social media platforms: 94 percent use YouTube, 80 percent use Facebook, 78 percent use Snapchat, 71 percent use Instagram, and 45 percent use Twitter.[2] The survey found that 51 percent of 18- to 24-year-olds stated that it would be "hard to give up" social media, compared to the population average of 40 percent.

In addition to using online platforms for social and recreational purposes, college students are increasingly using online learning tools as higher education moves from traditional lecture halls to the cloud. A 2019 *Inside Higher Ed* survey found that 46 percent of faculty taught an online course, up from 44 percent in 2018 and 30 percent in 2013.[3] When the COVID-19 pandemic forced campuses across the country to shut down, many universities transitioned to fully online learning. As faculty and students have rapidly adapted to new instructional tools, a shift toward sustained online learning in higher education will likely occur. The pandemic also produced new data privacy challenges, including those related to the use of online proctoring tools and COVID-19 monitoring technologies.

Because college students spend so much time and share so much information online, it is important to address the privacy issues that inevitably arise. Higher education institutions collect and use significant amounts of students' data in order to improve teaching, learning, advising, and other services that benefit students. Yet, research shows that college students often do not know how their institutions use their data,[4] and students are wary of privacy violations resulting from institutions' use of facial recognition, network monitoring, online learning, and predictive analytics systems. If students do not feel they can trust their education institutions' handling of personal data, then the institutions' data and technology-driven efforts may falter, regardless of any positive intent.

College students' privacy concerns also arise from their use of social media platforms, such as Snapchat, Instagram, and Facebook, and dating applications such as Tinder. Specific privacy risks include falling prey to deception, being a victim of doxing, and identity theft.

However, a pervasive societal belief is that young people care less about their data privacy than their parents or grandparents do.[5] A 2013 *USA Today* headline trumpeted, "Millennials don't worry about online privacy."[6] In August of 2020, *The Guardian* reported that young users of the popular social media app TikTok were "unfazed by US furor over data collecting," and the article quoted a Generation Z TikTok user who asked, "Am I the only one who doesn't care if China collects my data?"[7] In some cases, businesses and other data holders have used this perception to justify lax practices, by claiming that the younger generation finds current privacy protections to be sufficient. Yet, headlines proclaiming lack of privacy concerns often do not reflect how little evidence supports this assumption.

To better understand college students' views of data privacy, it is necessary to examine their opinions in their own voices. To do so, this paper identifies key themes and findings from interviews with and surveys of college-age young adults conducted between 2010 and 2021. In addition to asking how these groups feel about their data privacy generally, the interviews and surveys identify from which parties the respondents desire data privacy; the contexts in which they expect privacy; the factors impacting their expectations of privacy; whether certain subgroups have different privacy expectations; and the kinds of information they want to protect.

This report is organized into three subsequent sections. First, we outline our methodology, including the scope of our review, types of surveys and interviews reviewed, and limitations. Next, we identify the key findings of the review. Finally, the last section discusses implications of the findings and offers recommendations for additional data privacy research, policy, and practice.

METHODOLOGY

SCOPE

The Future of Privacy Forum conducted a review of publicly available quantitative and qualitative research on the privacy preferences, attitudes, and behaviors of college-age young adults in the United States and other countries. We examined both quantitative data, which provides insight into comparative preferences and changing attitudes of the population, and qualitative data, which reflects the considerations and nuances of individuals. Because research on US college students is limited, we included studies from other countries, including China, Germany, and Japan. We limited sources to the past decade, with most published in the past five years.

Surveys and Interviews

Although many informal surveys on consumers' attitudes towards privacy exist, this paper drew primarily from the most-respected organizations conducting public opinion polls in the US. We relied heavily on surveys conducted by the Pew Research Center and the Gallup Poll. Because Pew and Gallup generally polled the entire population and offered limited data on subgroups by age, we also examined surveys from EDUCAUSE and Kaplan, which focused more narrowly on higher education stakeholders. Moreover, the paper includes data from academic studies published in peer-reviewed journals, which provide more-specific and detailed data.

To complement the statistics, we also included qualitative data from interviews with focus groups. These peer-reviewed articles share college students' perspectives on privacy in their own words, providing rich preliminary findings.

Limitations

We found that data on the privacy attitudes of US college students is generally insufficient and inconclusive. As such, we expanded our scope and included data from studies conducted outside the US. Due to the scant privacy research conducted with college and university students, we also examined surveys that reported results by age, including data associated with the traditional age of college and university students (approximately 18–26). Further research is needed to reveal the diversity of privacy perspectives among and between college students from different age ranges and different countries.

Additionally, our limitation to publicly available data likely hindered the comprehensiveness of our review. Specifically, we were unable to access unpublished findings from internal focus groups or surveys commissioned by universities, foundations, governments, nonprofits, and corporations. This data can both inform internal decision-making and foster better public understanding of college students' data privacy attitudes. Restricted access to the data sets of general population surveys also presented a barrier. Because we could not analyze the data on a standard age range, we relied solely on reported age groups that aligned with the above-noted traditional age of college students.

Other limitations include the sample sizes from academic studies, which were often limited to participants from a single university. Findings from these studies therefore do not generalize beyond those institutional contexts. These limitations notwithstanding, the studies we examined provide compelling evidence of college students' attitudes, expectations, and behaviors regarding data privacy. We outline the key findings below.

KEY FINDINGS

Contrary to popular belief, college students care about their data privacy, and this concern is increasing.

A 2016 EDUCAUSE Center for Analysis and Research (ECAR) survey found that one-third of undergraduate students were "concerned that technology advances may increasingly invade [their] privacy."[8] A Gallup poll in 2015 found that 44 percent of millennials believe that their personal information is kept private "some of the time," and 26 percent believe that their personal information is kept private "little" or "none of the time."[9] In 2016, the Gallup poll showed that 44 percent of millennials trusted companies to keep their personal information private "all" or "most of the time," but 33 percent trusted companies to keep their personal information private "little" or "none of the time," a 7 percent increase from 2015.[10] These surveys reflect college students' growing awareness and distrust of entities possessing their data. In 2018, Gallup saw a 9 percent increase in respondents aged 18 to 49 who were "very concerned" about invasions of privacy when using Facebook, compared to 2011.[11]

A student respondent in the 2021 New America and National Association of Student Personnel Administrators (NASPA) focus group echoed this heightened attention and concern:

> "I'll say that I'm not as worried about my university taking my data. But I will say after watching The Social Dilemma on Netflix, I think that data usage is completely on my mind. Now. I still wouldn't say it's crippling. I don't, like, stay up every night thinking about it. But it's definitely more of [an] awakening of how much information is stored and how much is used on a daily basis."[12]

These studies and surveys indicate that college students are wary of privacy risks and value privacy protections. Yet, research also shows that they often behave in ways that put their and others' privacy at risk, a phenomenon called the "privacy paradox." A 2014 study of MIT undergraduates found that the students claimed to value privacy, but when offered a pizza, they readily disclosed the email addresses of three friends. According to the authors, "consumers deviate from their own stated preferences regarding privacy in the presence of small incentives, frictions and irrelevant information."[13]

Other research corroborates this view; a UK study of young adults' views of data privacy describes the general results of survey literature in the field of privacy: "Users, perhaps particularly young adults, report themselves to be very concerned about their online privacy and the flow of their personal information, yet upon examining their behaviour it seems they freely share personal information and either do not engage, or do not engage effectively, with privacy settings on social networking sites."[14] This contradictory behavior may result from various processes: users' "lack of technical skills and understanding required to protect" their online privacy; "moral panic," whereby users have no interest in their personal privacy; and the "optimistic bias," whereby "users are concerned about privacy on a societal level but do not consider themselves to be vulnerable and so do not feel the need to actively protect their privacy."[15]

Notwithstanding the observed privacy paradox, ample evidence suggests that college students take significant measures to protect their privacy. Lily, a student at the University of Texas at Austin, said that she carefully monitors which applications can access her information on Facebook: "If I end

up granting (an application) access, I make sure to change settings so it can't post things to my newsfeed automatically... It's important to me that I control exactly what is posted and what my friends will see from other applications."[16] Another 2018 Pew survey found that 44 percent of Facebook users aged 18 to 29 deleted the app from their phones in the previous year, and 64 percent changed their Facebook privacy settings. In comparison, only 12 percent of users above the age of 65 and 20 percent of users aged 50 to 64 deleted the Facebook app, and 33 percent of users above the age of 65 and 47 percent of users aged 50 to 64 adjusted their privacy settings.[17]

A qualitative study of American university students using Facebook also found that "the type of friend requests the participants accepted had changed over time. From accepting almost everyone requesting friendship, many participants reported having changed habits into being more restrictive about who they would accept." One 20-year-old female participant stated, "I was more open in the past [...if] I have no idea who they are I look at the mutual friends and then I will add them. Normally they will be: 'Ohh I met you here' and I will be like: 'Ohh yeah'. [...] If they are like: 'Hey I thought you were cute!' I will be like 'delete'!"[18] Nonetheless, the study found that although most participants had changed their Facebook privacy settings from the default, most were still unaware of who could access which information, and did not regularly manage or update their privacy settings.

College students want to protect information about their personal lives and their academic or professional prospects, but they prioritize the latter.

College students are particularly sensitive to how their online presence can impact their future opportunities. A study of undergraduate students at a midwestern university found that participants judged uses of their Facebook information for personal and direct marketing purposes to be less privacy-invasive, compared to uses for professional purposes related to hiring or promotion.[19] Another interview-based study at a midwestern university found that, when asked what they chose to post on Facebook, participants emphasized protecting their future employment prospects:

> An explicit concern was the impression they would make on future employers. This was one of the only specific concerns that were mentioned. This concern made the participants consider not only what they posted but also what friends posted on their wall and which pictures they were tagged in. Posting pictures and status updates including revealing pictures, illegal substances, and alcohol was in general for all participants a "no-go."[20]

In an informal survey conducted by *The Atlantic* in 2018 to understand how Cambridge Analytica impacted social media use, David, a young professional living in Boston, said of his social media activity, "Right off the bat I ... understood that anything you post on there can be seen pretty much by anyone at any time... So I don't really post anything at all. Anything that could be out there for public consumption, I try to manage very closely." He began self-censoring his social media posts after a friend's mother found pictures on Facebook showing him drinking while under age, and reported the behavior to his headmaster.[21] *The Atlantic* found that, of the 2,218 respondents, 82.2 percent self-censored on social media.

Other research confirms the effects of young people's social media use on their academic opportunities. In 2019, Kaplan's annual Test Prep survey of college admissions officers found that 59 percent viewed applicants' social media profiles as "fair game," and 32 percent said that what they saw negatively impacted their opinions of the applicants.[22]

At the same time, however, the 2018 version of the survey saw a three-year decline in the percentage

of admissions officers who viewed applicants' social media posts––a result partially attributed to difficulty finding applicants' social media accounts. According to Kaplan, 52 percent of the admissions officers say that "students have become savvier about hiding their social media presence over the past few years or moving away from social communities where what they post is easy to find by people they don't know."[23] Yariv Alpher, Kaplan's executive director of research, stated, "[Students] are more careful with what they post and are increasingly using more private social networks. In some cases they also create fake accounts that they only share with friends, but which are not easily attributed to

them."[24] A study examining privacy practices and attitudes among youth of low socioeconomic status confirmed this finding, as a 21-year-old participant named Beth stated, "You can't just say anything on the internet. I have to make sure that if anyone is interested in it and looks back at it [her various profiles], that they're not going to see anything that's going to ruin my life."[25]

This result may explain generational differences in use of social media platforms, as young people adapt to find their own spaces and compartmentalize the different aspects of their lives online. As parents and other authority figures become more active on social media, particularly Facebook, and monitor students' activities, young people feel compelled to move to other platforms where they can better protect their privacy. danah boyd, a researcher focusing on teenagers' use of social media, noted, "I see quotes over and over again from young people saying, 'Why are [adults on my social media site]? They don't belong here. Don't they understand?' Or, 'I wouldn't look at their content; why are they looking at mine?'"[26]

This insight suggests that while college students tend to prioritize privacy in their academic and professional lives, they still care deeply about protecting themselves from privacy violations outside of school and work. For example, most college-age Facebook users are friends with family members and other adults, such as teachers. Therefore, these users likely filter the information they post on Facebook, in contrast to other platforms. In the above-mentioned study of Facebook use among college students, "[m}ost participants were friends with family members and felt that if posted content was appropriate for family to see it was appropriate for everyone." A 20-year-old female participant stated, "I am friends with my mom on Facebook so I guess I am okay with my mom seeing it."[27]

Document dropping is an increasingly common form of cyber harassment about which young people express concern. This occurs when a digital antagonist gains access to personal documents––typically financial records, medical records, home addresses, phone numbers, or information about family members––and publishes them online. This practice is so pervasive that millennial and Gen Z users have dubbed it "doxing." High-profile doxing, such as the Gamergate scandal, has contributed to a sentiment of fear among young people online.[28] Aviva, a 23-year-old participant in the above-noted study by Marwick and colleagues, identified doxing as her greatest fear online. She is careful to keep a low profile on social media and is highly protective of information such as her address or phone number. In her words, "You see people getting doxed and that makes you realize how easy it is for people to get to your information. So you really do have to be very careful about who you talk to, and what you present online."[29]

Negative effects of college admissions officers and potential employers discovering compromising information on social media profiles are more likely than being the victim of doxing or identity theft. The outcome of the latter is much worse, however, as students may suffer constant psychological, emotional, and even physical harassment or bear the reputational, financial, and perhaps criminal costs of someone having stolen their identity. Young people express keen awareness of this personal risk.

College students expect boundaries between their personal and academic lives and want universities to use their data predominantly for educational (or health and safety) purposes.

A 2015 EDUCAUSE report on undergraduate students' views of information technology found that more than three-fourths of students approved of colleges' data collection for analytics when used for "progress toward [the student's] degree or certificate goal," and most approved of such collection for assessing course performance. However, less than half of the students approved of data collection to analyze students' campus-based activities logged through their IDs, smart cards, or smartphones; one-third approved of geolocation data collection; and one-quarter approved of data collection to analyze their social media activities.[30]

Another interview-based study by Jones et al. confirmed this preference, finding that students felt that universities' data collection was justified if the data was used only for educational purposes. One participant stated, "if they had the intention of using my data to create better programs or better educational tools, then I'm all for it."[31] Another participant supported this view: "I feel that if they're using data altruistically in a sense to better the experience for every student as a whole, then I feel that I can see it as a positive endeavor... a win for everybody."[32] However, the study also revealed that students were generally unaware of which information their schools collected and for what purposes.

As one student in New America and NASPA's focus groups stated, "I don't think I'm necessarily concerned about my institution's use of data privacy; I haven't really thought a lot about it. Because it's really not in my face often."[33] However, when questioned about their institutions' increased monitoring of students' locations for COVID-19-related health and safety purposes, students voiced privacy and equity concerns. One respondent noted, "It would sort of be very alarming to me [if my school traced my location]....I think in the era of COVID, we're asked that type of question on a daily [basis] of how much [privacy] are you willing to give away in order to maintain a sense of safety."[34] Another respondent also wanted their institution to enact guardrails for location data privacy: "There'd have to be a clear end. I wouldn't want that to continue after the pandemic so [there would need to be] transparency between the university and the students about when that data will stop being collected...and how they're getting rid of that information afterwards."[35]

Students expressed varying degrees of concern in the face of institutions' increased monitoring of students' social media activities, to ensure adherence to COVID-19 safety protocols. One student viewed it as "a complete violation," asserting, "Your private social media is your private social media,"[36] whereas others made an exception for health and safety reasons. As one student put it,

> I don't think it makes sense for them to go on social media, unless they have a case that has like been confirmed....I think if there's a party, and there's an instance where you need to have proof [or] you need to know who else was there, it might make sense to go on someone's account and ask their permission to see their account, if it's private. Otherwise, I don't really see why they need to be lurking on social media.[37]

Thus, even during the pandemic, which has blurred the lines between students' personal and academic lives, students expect institutions to respect their privacy and to commit to ethical, equitable data practices.

Mostly consistent with these findings, a 2016 German study reported that 82 percent of students agreed to share their course enrollment data, 78 percent agreed to share their learning strategies test results, and 75 percent agreed to share their mo-

tivation test results for learning analytics purposes. In contrast, 92 percent of students were unwilling to share their medical data, 91 percent were unwilling to share their income, 90 percent were unwilling to share their social media data, and 87 percent were unwilling to share their marital status.[38] This and the other studies noted above suggest that college students require a clear relationship between the information their institutions collect and its use for educational purposes.

Notably, most students were willing to share their social emotional learning survey results, which may be considered highly sensitive information, but were uncomfortable sharing much-less sensitive social media information. Therefore, the types of information college students seek to protect appears to depend heavily on the context of use, not solely the sensitivity of the information.

A survey of college students' perceptions of risk on Facebook and other online settings confirmed the importance of context. More than 90 percent of the survey's 3,000 respondents listed their full names on Facebook, approximately 70 percent listed their birth date, approximately 70 percent listed their email address, more than 85 percent listed their hometowns, and almost 100 percent posted photos of themselves. However, only 10–14 percent listed their current address, and less than 30 percent listed their current phone number.[39] While differing norms of engagement exist in schools and on social media, the question remains why college students choose to share certain information in some contexts and not others. Thus, further research on the differences between acceptable disclosure in academic and personal settings is necessary.

College students care more about protecting immutable identifiers, such as biometric information, in higher education contexts.

Unfortunately, research is lacking on which personal identifiers US college students believe require the most protection. However, studies suggest that college students prioritize protecting immutable identifiers, such as biometric information, from their education institutions. A comparative study of college students in China and Japan found that in an e-learning context, students considered their personal photos, mobile phone numbers, and physical addresses to be very private and were reluctant to submit this information to e-learning systems. However, they did not consider age, personal URLs, birthplace, instant messenger IDs, or email addresses to be sensitive information.[40]

Students have also mobilized to prevent schools and governments from adopting privacy-invasive systems that use biometric information. Erica Darragh, a student at the University of North Georgia, is part of a campaign to ban facial recognition on college campuses. In an article published on *Vice*, she wrote,

> We have already given up so much privacy and liberty for the sake of "security," but facial recognition must be where this stops. Facial recognition does not improve security and may actually make it worse. It's also a technology that, once mainstreamed, can never be taken back. It is fundamentally coercive for educational institutions to require students to participate in biometric surveillance in order to attend class. While we wait for the government to ban facial recognition at the federal level, young people can take control of the narrative and demand policies that ban the technology in school districts and on college campuses.[41]

In 2020, in response to a proposal to adopt facial recognition for security surveillance at UCLA, students from 36 schools protested, in person and via online petitions, universities' use of facial recognition systems. The pushback from students and the community led UCLA and about 50 other schools to promise not to use facial recognition technology on their campuses.[42]

Some personal identifiers are easily replaced, or people can possess many of them, such as email addresses. In contrast, biometric information, such as facial, retinal, or fingerprint scans, is singular and irreplaceable. College students' strong belief in protecting immutable identifiers thus likely stems from their desire to shield themselves from privacy risks and harms that may follow them for the rest of their lives.

College students have greater confidence that education institutions and the government will protect their privacy, compared to technology companies.

A 2016 Gallup poll found that 19 percent of millennials had "a lot of trust" in the federal government to safeguard their personal data, 18 percent trusted their state governments to do so, and only 4 percent trusted social networking websites or applications to do so.[43] An annual survey conducted by the Center for the Digital Future, at USC Annenberg, found that in 2018, for five consecutive years respondents expressed greater concern about corporations violating their privacy (57 percent) than about governments (52 percent) or other people (47 percent) doing so.[44] More recently, a January 2021 survey conducted by The Generation Lab found that 51 percent of college students believe that the government should regulate major tech companies more, and 77 percent believe that social media companies have too much power and influence in politics today.[45]

A Knight Foundation and Gallup survey reflects this negative view of technology companies, finding that 77 percent of American respondents believe that companies such as Google, Facebook, Amazon, and Apple have "too much power." Only 1 percent thought that technology companies have "too little power."[46] However, compared to older respondents, fewer younger respondents between the ages of 18 and 34 viewed companies as "creating more problems than they solve."[47] Younger respondents were also more comfortable with technology companies using their personal information, as 37 percent reported feeling very uncomfortable with the practice. Among older respondents, 40 percent aged 35 to 54 and 48 percent over the age of 55 stated they were very uncomfortable with companies using their personal information.[48]

This disparity of trust in companies compared to the government does not stem from a belief that the government does not collect or collects less personal information from citizens. The 2018 Pew survey found that about 60 percent of respondents aged 18 to 29 believe that the government tracks their online and cellphone activities, and 30 percent believe that the government tracks their offline activities.[49] The difference seems to lie in perceptions of how the governments and companies will use the information, as governments exist to serve people, whereas companies are obligated to their shareholders.

With regard to education institutions, a New America and NASPA study participant expressed a high level of trust and confidence in their institution:

> "I would definitely say I'm less concerned about my institution collecting data. Because they generally don't ask for data a whole lot of the time, besides what they get from, like the basic application type stuff. And I think FERPA just makes me feel better, because it's like federal law. And as a student in higher ed who has worked in very FERPA protected areas, it's very much like, FERPA is a big deal. Institutions are really, in my opinion, going the extra mile to protect student data."[50]

This respondent found reassurance in their awareness of federal regulations requiring student privacy rights and protections, such as the Family Educational Rights and Privacy Act (FERPA). However, respondents did not express similar sentiments about commercial or government use of students' data, suggesting that students might have greater confidence in companies and governments if policies similar to FERPA governed data practices outside of education settings.

Participants in the Jones et al. study also clearly differentiated their privacy expectations of companies as opposed to education institutions. One student stated, "I personally trust schools and universities more than these companies that are for-profit and I trust that they're going to use this information in a way that I feel more comfortable with, that doesn't try to take money out of my pocket."[51] The participants believed that universities have students' best interests at heart and therefore deserve their trust regarding the collection and use of their information, compared to businesses such as Facebook and Amazon, which seek to profit from consumers' data. This finding reflects a tendency to trust public

institutions more than private companies. However, more surveys are needed that compare college students' views of their personal information in the hands of their universities compared to the government and companies.

While students generally trust their universities, they still have questions about the utility and reliability of the information universities collect. In a 2016 Australian study of students' attitudes toward learning analytics in higher education, a student wondered about the accuracy of the information collected via the school's learning management system (LMS): "there's information how long you've been on Blackboard and how [sic] the books you got out. There—– there's like a risk of the data not being accurate."[52] This student conveyed a concern that the activity measured, specifically time spent on the LMS and books borrowed, does not accurately reflect active learning. If students are to believe that universities' collection and use of their personal information is justified in order to improve their educational experiences, students seem to want proof that the information collected reliably serves this purpose.

Students are particularly concerned about how their institutions use predictive analytics data to determine future possibilities. A US case study revealed that students were frustrated by learning and early advising management systems that used predictive data to recommend course pathways, because they believed the systems used incomplete or inaccurate data to discourage them from courses or majors that interested them. One student stated, "Who can decide my future beside myself? I would ignore this kind of information" and "Don't tell me what I can or can't do."[53] However, the same study revealed that students supported predictive analytics that provided opportunity, such as by matching current majors or skills to potential career paths. Most importantly, students wanted to receive support from trusted faculty or advisors with whom they had a foundation of trust.

ECAR's 2019 survey of US students found that 70 percent expressed confidence in their university's ability to safeguard their personal data. However, only 45 percent believed they benefited from their university's privacy and security policies, and 44 percent reported understanding how their university used their personal data.[54] A three-part study of UK university students' expectations of learning analytics concluded that students feel very strongly that their universities should safeguard their educational data, and "want to be reassured that their data are secure and private."[55] The study also found that students expect their universities to obtain informed consent to use and outsource their identifiable data to third-party companies. This reveals that students' trust in universities does not mean unlimited and unrestricted access. Rather, college students expect a higher standard of information privacy and security in return for their trust.

Students also voiced concerns about equity and bias, specifically the potential to be treated differently based on certain parties gaining access to their personal information. Another respondent in the Australian study worried that, "if a teacher can see your grades they might just pay attention to the one who's getting high grades and not everyone else."[56] Therefore, college students expect universities to ensure equitable outcomes, in addition to exercising transparency and accountability in the collection, use, and disclosure of student information.

IMPLICATIONS & RECOMMENDATIONS

Students' perceptions of and attitudes toward data privacy will shape the future architecture and policies that govern the internet. Today's college and university students are living in environments that increasingly require regular interaction with data and technology. Some of these students have or will soon enter the workforce as software engineers, tech startup entrepreneurs, journalists, and in other professions integral to collective privacy conversations. According to the National Center for Education Statistics (NCES), 71,420 students graduated with degrees in computer and information sciences in 2017, up from 64,402 in 2016 and 59,271 in 2015. In 2017, 381,353 students also graduated with degrees in business, and 93,776 students graduated with degrees in communications, journalism, and related programs.[57] These graduates will bring their attitudes about data privacy to their new careers, and these attitudes will influence the questions they ask and the decisions they make. The following three recommendations can help education and privacy stakeholders develop and shape college and university students' data privacy expectations and practices.

1. Higher education institutions should teach data privacy, ethics, and literacy courses to encourage college students to think critically about data privacy.

Research demonstrates that students care about privacy, but knowledge of the depth and breadth of their awareness is still lacking. The higher education system must prepare students to fully comprehend the implications of the collection, use, and sharing of their personal information without their knowledge and consent. The US education system was built to develop an informed citizenry able to participate in a democracy. Now more than ever, students need to understand the factors that shape their opinions and influence their decisions. Helping students understand how data is collected and used, as well as how they can protect their personal information and actively engage the platforms collecting and the policies governing their data, is vital to this goal.

To keep pace with societal and technological developments and cultivate data-literate citizens, higher education should develop curricula that include instruction on data privacy and ethics. The benefits of this instruction are clear. In an article published in the *Stanford Daily*, undergraduate student Trisha Kulkarni shared her reflections on taking the course Computer Science, Ethics, and Policy: "By the end of the class, I was overwhelmed at the details I had overlooked in my daily practices, such as clicking 'accept' without reading a privacy notice or continuously giving an app or website information about my interests in order to customize my experience."[58] Practitioners, scholars, and policymakers should also collaborate to design data ethics curricula.

2. To foster trust and cooperation, higher education institutions and technology companies should communicate how and why they collect and use students' personal information.

Research reveals that students lack awareness of the data collection, maintenance, use, and disclosure practices of their colleges and universities and are wary of institutions using their information for non-educational purposes. Unless effectively communicated to students and communities, good privacy policies and practices can still result in general mistrust and apprehension. In a recent analysis of US higher education privacy policies,[59] researchers

found that policy language often ineffectively conveys how institutions use data. As a result, current policies can cause students to misunderstand their institutions' data practices and limit their ability to engage with, correct, or opt out of those practices.

Higher education institutions should collect and use only the information necessary to fulfill goals related to understanding and improving students' educational outcomes and well-being. Institutions should also convene town halls, organize student advisory boards, hold office hours, and publish clear explanations of how and why they collect and use students' personal information. They should share these policies on institutional websites in plain language that clearly communicates the methods that students can use to review, change, or opt out of data collection. Moreover, because third-party technology companies often mediate higher education organizations' data use, these companies should also be transparent about their processes, scope, and intent of data collection, analysis, and use.

3. Organizations should release additional findings on college students' attitudes toward privacy, and researchers should conduct more studies on specific privacy topics.

To verify and extend the findings we have outlined, researchers and organizations should conduct more studies of students' attitudes about privacy. The field would greatly benefit if Pew, Gallup, and other organizations conducted public opinion polls on privacy concerns, with subgroup data reported by age, including a narrow range of traditional ages of college and university students (18- to 26-year-old students). Rather than privacy researchers and stakeholders attempting to replicate such well-designed surveys, the organizations holding the data should consider releasing their information tailored to the target population.

The following recommended topics for further research would also provide greater insight into US college students' attitudes toward privacy.

How do college students' privacy attitudes differ based on race, ethnicity, socioeconomic status, special needs, citizenship status, gender, and so forth?

Some advocates argue that new technologies, particularly artificial intelligence systems relying on algorithms that have been criticized for demonstrating racial and gender bias, disproportionately harm students of color and other marginalized student groups. Surveys also find that communities of color express greater privacy concerns, as 60 percent of black Americans believe that the government tracks all or most of their online activities, compared to 43 percent of white Americans. Black Americans are also more likely to suffer from privacy harms. The Pew Research Center reported that 20 percent of black respondents said that "someone has taken over their social media or email account in the past year," compared to 7 percent of Hispanic respondents and 6 percent of white respondents.[60]

Therefore, research is needed to better understand how students from subgroups that have historically faced discrimination perceive privacy concerns, compared to other subgroups. The aforementioned Marwick study focused on young people of low socioeconomic status from an urban metropolis, providing valuable insight into the privacy practices and attitudes of this subgroup. Other marginalized groups can benefit from similar studies. For example, how do African American students, undocumented students, and students receiving mental health care feel about their privacy protections? How do the intersections of different identities influence these privacy attitudes?

Which types of personal information do college students want to protect, and from whom?

The studies cited in this paper demonstrate that privacy expectations depend heavily on context. College students may perceive that certain information is highly sensitive and requires stringent privacy protections when universities hold the data, but in the context of social media platforms, they may not believe the same information merits the same level of protection. However, research is lacking on which types of information college students believe should be protected in academic, social, and professional settings. There is a need for more studies about students' understandings of different types of data, which types they believe require greater privacy protections, and why.

Future studies should also explore college students' expectations of privacy regarding particular types of information from particular entities. The above-noted study of East Asian students' attitudes about data privacy in the context of e-learning provides a foundation for similar studies in the United

States. There is also a need for comparative studies measuring people's evaluations of the same types of information held or accessed by different entities. For example, how do students rank the sensitivity of different types of personal information, such as name, address, photo, geolocation data, and friend lists, when held by universities as opposed to parents, the government, or businesses?

Which sources and events influence the privacy attitudes of college students?

Current events, scandals, and revelations influence public attitudes toward data privacy issues, but research on the processes and events shaping college students' attitudes towards privacy is lacking. Focus groups and surveys therefore should study the factors affecting students' awareness and expectations of privacy. For example, which sources influence college students the most: traditional media, social media, or word of mouth? Which past events have most impacted college students' perceptions of privacy? Studies could address how college students' privacy attitudes have changed in the aftermath of events such as the Edward Snowden disclosures, the Cambridge Analytica scandal, and the COVID-19 pandemic.

Stakeholders also need to better understand these sources in order to prevent manipulation of college students' privacy attitudes. For example, misinformation about privacy concerns may lead students to either accept inadequate privacy protections or reject responsible ones. Proper oversight and prevention of such media manipulation require a thorough understanding of the sources.

How do college students' privacy attitudes change over time?

New technological and legal developments and greater media attention have contributed to rapidly changing perceptions of privacy. Yet, no longitudinal studies have tracked college students' attitudes toward privacy over time. Because society is at a critical juncture regarding approaches to and norms of data privacy, longitudinal studies would provide valuable information to help privacy stakeholders shape these approaches and norms. A study modeled on the well-known Study of Adult Development, which for the past 80 years has followed two groups of men, one composed of Harvard graduates from the classes of 1939 to 1944 and the other composed of men who grew up in inner-city Boston,[61] would provide valuable data for the field of privacy research.

CONCLUSION

Leaders at higher education institutions increasingly rely on data collected from students to inform decision making, and they employ technology platforms that allow them to collect, analyze, and use vast amounts of this data. As students have become more aware of this ongoing data collection and use, they have begun to express their concerns and desires to limit the use of their data to guide institutional decision making. The conversation about the use and privacy of students' data has just begun, and students' voices need to be privileged in that conversation. Higher education institutions, technology companies, researchers, other interested stakeholders *and students* can collectively shape the future of data privacy in higher education.

ENDNOTES

1 The authors thank the numerous people who contributed to this report, particularly Larissa Kehne, Preeti Jain, Dr. Carrie N. Klein, and Ashleigh Imus.
2 Aaron Smith and Monica Anderson, *Social Media Use in 2018*, Pew Research Center, (March 1, 2018), Accessed April 5, 2020, https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/.
3 Doug Lederman, *Professors' Slow, Steady Acceptance of Online Learning: A Survey*, Inside Higher Ed, (October 30, 2019), Accessed April 5, 2020, https://www.insidehighered.com/news/survey/professors-slow-steady-acceptance-online-learning-survey.
4 Joseph Galanek and Ben Shulman, *Not Sure If They're Invading My Privacy or Just Really Interested in Me*, EDUCAUSE Review, (December 11, 2019), Accessed April 5, 2020, https://er.educause.edu/blogs/2019/12/not-sure-if-theyre-invading-my-privacy-or-just-really-interested-in-me.
5 See, for example, David Erickson, *Millennials Don't Care About Privacy,* e-Stategy Trends, (September 8, 2017), Accessed July 22, 2021, https://trends.e-strategyblog.com/2017/09/08/millennials-dont-care-privacy/28667/; Kari Paul, *'I don't care': young TikTokers unfazed by US furor over data collection,* The Guardian, (August 5, 2020), Accessed July 22, 2021, https://www.theguardian.com/technology/2020/aug/05/tiktok-gen-z-millennials-data-privacy-trump-china; Sarah Landrum, *Millennials, Trust, And Internet Security,* Forbes, (June 28, 2017), Accessed July 22, 2021, https://www.forbes.com/sites/sarahlandrum/2017/06/28/millennials-trust-and-internet-security/?sh=5187c95e5555; John H. Fleming and Amy Adkins, *Data Security: Not a Big Concern for Millennials,* Gallup, (June 9, 2016, Accessed July 22, 2021, https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx; Matthew Hennessey, *Why millennials will learn nothing from Facebook's privacy crisis,* New York Post, (April 7, 2018), Accessed July 22, 2021, https://nypost.com/2018/04/07/why-millennials-will-learn-nothing-from-facebooks-privacy-crisis/; Robert Williams, *Study: Gen Z opts for personalized, interactive content over privacy,* Marketing Dive, (June 4, 2019), Accessed July 22, 2021, https://www.marketingdive.com/news/study-gen-z-opts-for-personalized-interactive-content-over-privacy/556101/; Hunter Schwarz, *Millennials are a little confused when it comes to privacy,* The Washington Post, (May 13, 2015), Accessed July 22, 2021, https://www.washingtonpost.com/news/the-fix/wp/2015/05/13/millenials-dont-trust-government-to-respect-their-privacy-but-they-do-trust-businesses-what/.
6 Hadley Malcom, *Millennials don't worry about online privacy,* USA Today, (April 21, 2013), Accessed July 22, 2021, https://www.usatoday.com/story/money/business/2013/04/21/millennials-personal-info-online/2087989/.
7 Kari Paul, *'I don't care': young TikTokers unfazed by US furor over data collection,* The Guardian, (August 5, 2020), Accessed July 22, 2021, https://www.theguardian.com/technology/2020/aug/05/tiktok-gen-z-millennials-data-privacy-trump-china.
8 D. Christopher Brooks, *ECAR Study of Undergraduate Students and Information Technology*, EDUCAUSE, (2016), Accessed April 5, 2020, https://er.educause.edu/~/media/files/library/2016/10/ers1605.pdf?la=en, 22.
9 John Fleming, *Millennials Most Trusting on Safety of Personal Information*, Gallup, (May 11, 2015), Accessed April 5, 2020, https://news.gallup.com/poll/183074/millennials-trusting-safety-personal-information.aspx.
10 John H. Fleming and Amy Adkins, *Data Security: Not a Big Concern for Millennials*, Gallup, (June 9, 2016), Accessed April 5, 2020, https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx.
11 Jeffrey M. Jones, *Facebook Users' Privacy Concerns Up Since 2011*, Gallup, (April 11, 2018), Accessed April 5, 2020, https://news.gallup.com/poll/232319/facebook-users-privacy-concerns-2011.aspx.
12 Jill Dunlap, Iris Palmer, and Alexa Wesley, *Keeping Student Trust: Student Perceptions of Data Use Within Higher Education,* New America, (March 10, 2021), Accessed April 12, 2021, https://www.newamerica.org/education-policy/reports/keeping-student-trust/.
13 Susan Athey, Christian Catalini, and Catherine Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, NBER Working Paper Series (June 2017), Accessed April 5, 2020, https://www.nber.org/papers/w23488.pdf, 4.
14 Michael Dowd, *Contextualized Concerns: The Online Privacy Attitudes of Young Adults,* International Federation for Information Processing, (2011), Accessed April 5, 2020, https://link.springer.com/content/pdf/10.1007/978-3-642-20769-3_7.pdf, 79–80.
15 Ibid, 80.
16 Katey Psencik, *How much do college students care about online privacy?*, USA Today, (May 29, 2013), Accessed April 5, 2020, https://www.usatoday.com/story/news/nation/2013/05/29/college-students-online-privacy-debate/2369941/.
17 Andrew Perrin, *Americans are changing their relationship with Facebook*, Pew Research Center, (September 5, 2018), Accessed April 5, 2020, https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.
18 Nis Bornoe and Louise Barkhuus, *Privacy Management in a Connected World: Students' Perception of Facebook Privacy Settings*, Conference on Computer Supported Cooperative Work, (2011), Accessed April 5, 2020, https://www.bornoe.org/papers/CSCW2011-Collaborative-Privacy-Workshop-bornoe.pdf.
19 Katherina Glac, Dawn R. Elm, and Kirsten Martin, *Areas of Privacy in Facebook: Expectations and Value*, Business & Professional Ethics Journal (2014), 33 (2/3): 147–176, Accessed April 5, 2020, https://www.jstor.org/stable/44074811.
20 Nis Bornoe and Louise Barkhuus, *Privacy Management in a Connected World: Students' Perception of Facebook Privacy Settings*, Conference on Computer Supported Cooperative Work, (2011), Accessed April 5, 2020, https://www.bornoe.org/papers/CSCW2011-Collaborative-Privacy-Workshop-bornoe.pdf.
21 Julie Beck, *People Are Changing the Way They Use Social Media*, The Atlantic, (June 7, 2018), Accessed April 5, 2020, https://www.theatlantic.com/technology/archive/2018/06/did-cambridge-analytica-actually-change-facebook-users-behavior/562154/.
22 Kaplan, *Kaplan Survey: Percentage of College Admissions Officers Who Visit Applicants' Social Media Pages on the Rise Again*, Kaplan, (January 13, 2020), Accessed April 5, 2020, https://www.kaptest.com/blog/press/2020/01/13/kaplan-survey-percentage-of-college-admissions-officers-who-visit-applicants-social-media-pages-on-the-rise-again/.
23 Kaplan, *Kaplan Test Prep Survey: Social Media Checks By College Admissions Officers Decline Due to Savvier Applicants and Shifting Attitudes*, Kaplan, (November 27, 2018), Accessed April 5, 2020, https://www.kaptest.com/blog/press/2018/11/27/kaplan-test-prep-survey-social-media-checks-by-college-admissions-officers-decline-due-to-savvier-applicants-and-shifting-attitudes-2/.
24 Ibid.
25 Alice Marwick, Claire Fontaine, and danah boyd, *"Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth*, Social Media + Society, (May 2017), Accessed April 5, 2020, https://doi.org/10.1177/2056305117710455.
26 Knowledge@Wharton, *Teens Are Waging a Privacy War on the Internet — Why Marketers Should Listen*, Knowledge @ Wharton, (August 5, 2014), Accessed April 5, 2020, https://knowledge.wharton.upenn.edu/article/teens-privacy-online/.
27 Nis Bornoe and Louise Barkhuus, *Privacy Management in a Connected World: Students' Perception of Facebook Privacy Settings*, Conference on Computer Supported Cooperative Work, (2011), Accessed April 5, 2020, https://www.bornoe.org/papers/CSCW2011-Collaborative-Privacy-Workshop-bornoe.pdf.
28 Simon Parkin, *Gamergate: A Scandal Erupts in the Video-Game Community*, The New Yorker, (October 17, 2014), Accessed April 5, 2020, https://www.newyorker.com/tech/annals-of-technology/gamergate-scandal-erupts-video-game-community.
29 Alice Marwick, Claire Fontaine, and danah boyd, "*Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth*, Social Media + Society, (May 2017), Accessed April 5, 2020, https://doi.org/10.1177/2056305117710455.

30 Eden Dahlstrom, D. Christopher Brooks, Susan Grajek, and Jamie Reeves, *ECAR Study of Undergraduate Students and Information Technology, 2015*, EDUCAUSE, (2015), Accessed April 5, 2020, https://library.educause.edu/-/media/files/library/2015/8/ers1510ss.pdf?la=en&hash=5B932D434EF273031FC601C538D52D7524017682.

31 Kyle M.L. Jones, Andrew Asher, Abigail Goben, Michael R. Perry, Dorothea Salo, Kristin A. Briney, and M. Brooke Robertshaw, *"We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education*, Journal of the Association for Information Science and Technology, (April 2020), Accessed April 6, 2020, https://doi.org/10.1002/asi.24358, 15.

32 Ibid.

33 Jill Dunlap, Iris Palmer, and Alexa Wesley, *Keeping Student Trust: Student Perceptions of Data Use Within Higher Education,* New America, (March 10, 2021), Accessed April 12, 2021, https://www.newamerica.org/education-policy/reports/keeping-student-trust/.

34 Ibid.

35 Ibid.

36 Ibid.

37 Ibid.

38 Dirk Ifenthaler and Clara Schumacher, *Student perceptions of privacy principles for learning analytics,* Educational Technology Research and Development (2016), 64: 923–938, https://link.springer.com/article/10.1007/s11423-016-9477-y.

39 Kayla Picotte, *Personal Information in Public Domain: Perceptions of Risk Among College Students on Facebook and the Outside World*, Master's Thesis, University of North Carolina Wilmington, (2012), Accessed April 5, 2020, http://dl.uncw.edu/Etd/2012-1/picottek/kaylapicotte.pdf, 26.

40 Fang Yang and Shudong Wang, *Students' Perception Toward Personal Information and Privacy Disclosure in E-Learning*, The Turkish Online Journal of Educational Technology, (January 2014), Accessed April 5, 2020, https://pdfs.semanticscholar.org/027e/e162b8526aef855b0f7e0132d61140fcb3a7.pdf.

41 Erica Darragh, *Here's Why I'm Campaigning Against Facial Recognition in Schools*, VICE, (March 11, 2020), Accessed April 5, 2020, https://www.vice.com/en_us/article/z3bgpj/heres-why-im-campaigning-against-facial-recognition-in-schools.

42 Kari Paul, *'Ban this technology': students protest US universities' use of facial recognition*, The Guardian, (March 2, 2020), Accessed April 5, 2020, https://www.theguardian.com/us-news/2020/mar/02/facial-recognition-us-colleges-ucla-ban.

43 John H. Fleming and Amy Adkins, *Data Security: Not a Big Concern for Millennials*, Gallup, (June 6, 2016), Accessed April 5, 2020, https://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx.

44 2018 Digital Future Project, *Surveying the Digital Future: The 16th annual study on the impact of digital technology on Americans*, Center for the Digital Future at USC Annenberg, (2018), Accessed April 5, 2020, https://www.digitalcenter.org/wp-content/uploads/2018/12/2018-Digital-Future-Report.pdf, 89.

45 The Generation Lab, *Youth Dems and GOP love tech and want it to stop*, The Generation Lab, (January 28, 2021), Accessed February 3, 2021, https://www.generationlab.org/post/youth-dems-and-gop-love-tech-and-want-it-to-stop.

46 The John S. and James L. Knight Foundation and Gallup, *Techlash? America's Growing Concern With Major Technology Companies*, Knight Foundation and Gallup, (2020), Accessed April 5, 2020, https://knightfoundation.org/wp-content/uploads/2020/03/Gallup-Knight-Report-Techlash-Americas-Growing-Concern-with-Major-Tech-Companies-Final.pdf, 13.

47 Ibid, 5.

48 Ibid, 19.

49 Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (November 15, 2019), Accessed April 5, 2020, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

50 Jill Dunlap, Iris Palmer, and Alexa Wesley, *Keeping Student Trust: Student Perceptions of Data Use Within Higher Education,* New America, (March 10, 2021), Accessed April 12, 2021, https://www.newamerica.org/education-policy/reports/keeping-student-trust/.

51 Kyle M.L. Jones et al., *"We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education*, Journal of the Association for Information Science and Technology, (April 2020), Accessed April 6, 2020, https://doi.org/10.1002/asi.24358, 17.

52 Lynne D. Roberts, Joel A. Howell, Kristen Seaman, and David C. Gibson, *Student Attitudes toward Learning Analytics in Higher Education: "The Fitbit Version of the Learning World,"* Frontiers in Psychology (2016), https://www.frontiersin.org/article/10.3389/fpsyg.2016.01959.

53 Carrie Klein et al., *Student Sensemaking of Learning Analytics Dashboard Interventions in Higher Education*, Journal of Educational Technology Systems (2019), 48 (1): 130–154, https://journals.sagepub.com/doi/full/10.1177/0047239519859854.

54 Joseph Galanek and Ben Shulman, *Not Sure If They're Invading My Privacy or Just Really Interested in Me*, EDUCAUSE Review, (December 11, 2019), Accessed April 5, 2020, https://er.educause.edu/blogs/2019/12/not-sure-if-theyre-invading-my-privacy-or-just-really-interested-in-me.

55 Alexander Whitelock-Wainwright, Dragan Gasevic, Ricardo Ejeiro, Yi-Shan Tsai, and Kate Bennet, *The Student Expectations of Learning Analytics Questionnaire*, Journal of Computer Assisted Learning (October 2019), Vol 35, Issue 5, https://doi.org/10.1111/jcal.12366.

56 Lynne D. Roberts, Joel A. Howell, Kristen Seaman, and David C. Gibson, *Student Attitudes toward Learning Analytics in Higher Education: "The Fitbit Version of the Learning World*," Frontiers in Psychology (2016), Accessed April 5, 2020, https://www.frontiersin.org/article/10.3389/fpsyg.2016.01959.

57 National Center for Education Statistics, *Table 332. 10. Bachelor's degrees conferred by postsecondary institutions, by field of study: Selected years, 1970-71 through 2016-17*, NCES, (August 2018), Accessed April 5, 2020, https://nces.ed.gov/programs/digest/d18/tables/dt18_322.10.asp.

58 Trisha Kulkarni, *Making Privacy Public*, The Stanford Daily, (January 15, 2020), Accessed April 5, 2020, https://www.stanforddaily.com/2020/01/14/making-privacy-public/.

59 Michael Brown and Carrie Klein, *Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents*, The Journal of Higher Education, (June 22, 2020), Accessed November 10, 2020, https://www.tandfonline.com/doi/abs/10.1080/00221546.2020.1770045.

60 Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, (November 15, 2019), Accessed April 5, 2020, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

61 Massachusetts General Hospital and Harvard Medical School, *Study of Adult Development, History of the Study*, Massachusetts General Hospital and Harvard Medical School, (2015), Accessed April 30, 2020, https://www.adultdevelopmentstudy.org/grantandglueckstudy.


FUTURE OF
PRIVACY
FORUM