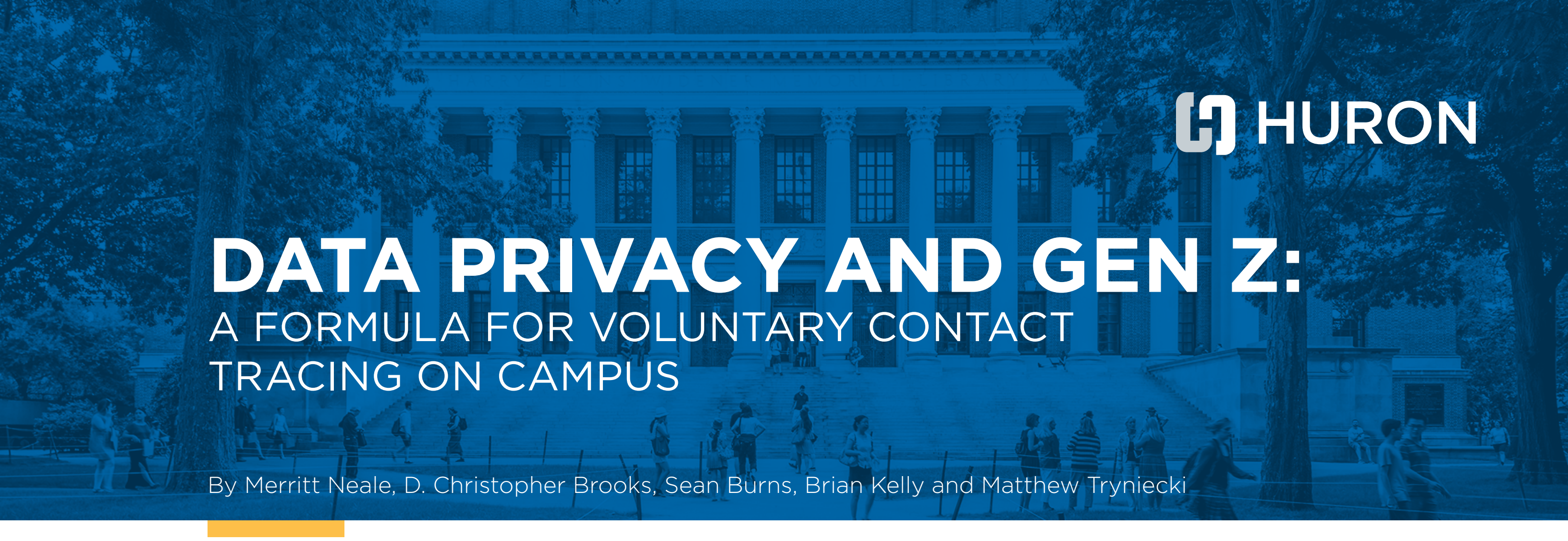


HURON

DATA PRIVACY AND GEN Z:

A FORMULA FOR VOLUNTARY CONTACT TRACING ON CAMPUS

By Merritt Neale, D. Christopher Brooks, Sean Burns, Brian Kelly and Matthew Tryniecki

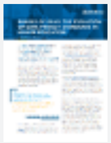
In the state of heightened awareness about safety and security that has emerged as a byproduct of the COVID-19 pandemic, colleges and universities are seeking to strike a balance between promoting public health and ensuring student privacy. While many federal and state agencies allow for the relaxing of certain regulations in emergencies, the line between duty of care and student privacy is often blurred.

Contact tracing is widely considered to be one of the best methods for safe reopening, yet there are concerns the technology that enables this capability may be used to infringe upon technical and administrative privacy safeguards. In fact, a Brookings Institute survey of 2,000 Americans found that only 30% of respondents felt comfortable downloading and using a mobile contact tracing app, with support increasing alongside stronger privacy protections.

What Is Contact Tracing?

> "Contact tracing is used by health departments to prevent the spread of infectious disease. In general, contact tracing involves identifying people who have an infectious disease (cases) and people who they came in contact with (contacts) and working with them to interrupt disease spread."
>
> — Centers for Disease Control and Prevention (CDC)

Shades of Gray: The Evolution of Data Privacy Standards in Higher Education



Forward-thinking institutions are embracing a new frontier in higher education by building the robust infrastructure required to support ethical data usage. Read more.

In 2020, EDUCAUSE conducted a survey of 16,162 students from 71 U.S. institutions[1] (full results will be reported via EDUCAUSE's website in the fall of 2020) and found that students' perceptions of data privacy varied widely, though the majority reported confusion over how their data are used and skepticism about their institution's ability to ethically protect their personal information (see table below). EDUCAUSE's most recent list of the top 10 information technology (IT) issues similarly identified privacy as a major concern for higher education leaders, coming in at No. 2, just behind information security strategy.

[1] For the 2020 EDUCAUSE Student Survey, only data collected during the pre-pandemic period (January 14, 2020, through March 11, 2020) are reported here. An additional 9,477 student responses were collected between March 12, 2020, and June 1, 2020, but are excluded from this analysis.

2020 EDUCAUSE Student Technology Survey Results

Please tell us how much you agree or disagree with the following statements about your institution's collection, protection, and use of personal data:

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
I trust my institution to use my personal data ethically and responsibly.	8%	10%	31%	38%	13%
I have confidence in my institution's ability to safeguard my personal data.	8%	11%	33%	35%	12%
I benefit from my institution's collection and use of my personal data.	9%	17%	44%	23%	8%
I understand how my institution uses my personal data.	21%	33%	23%	18%	6%

With over 50% of students reporting a lack of understanding of how their institution uses their personal data, the key to managing the community's perspectives on contact tracing lies in proactive, transparent, trust-building communication that ensures all stakeholders are aware of the ways their data are being collected and used as well as the precautions the institution is taking to ensure anonymity and data security. It is also critical that higher education leaders seek to highlight the tangible benefits of safely reopening campuses via contact tracing to create a value proposition that students and their families can easily understand and support.

Demonstrating a Commitment to Privacy and Ethical Data Usage

EDUCAUSE's 2020 Student Technology Survey found that only slightly over half of respondents agreed or strongly agreed that they trusted their institutions to use their data ethically. The survey also found that fewer than half of students had confidence (choosing either agree or strongly agree) in their institutions' ability to safeguard their personal data. This is indicative of the fact that Generation Z may be more concerned about data privacy and security than Millennials, adjusting their privacy settings much more frequently than their generational neighbors.

EDUCAUSE's Seven Digital Ethics Questions for Higher Ed Leaders

Although data privacy has been flagged as a top concern, how do you think your campus leadership would respond to these questions? Consider these seven questions as a way to assess your institution's maturity around digital ethics.

1. Is there a community of concern related to digital ethics on your campus?
2. Does your campus have written policies or guidelines related to privacy and digital ethics? Can you find them?
3. Do you know whose full-time job it is to worry about ethical issues?
4. When someone on campus develops an application that uses student data, is any ethical framework used before work begins?
5. When someone on campus buys an application, is there any ethical review required?
6. Do you know what your campus is doing to ensure that the next generation of developers and technology professionals (our students) has a strong digital ethics mindset?
7. Are you more informed about digital ethics this year than last? Will you be even more informed next year? How will you make this happen with everything else going on?

This generation's consistent use of Snapchat, Instagram and other social media has made posting personal information online (inadvertently or intentionally) a part of their everyday lives. Thus, the need for open, transparent communication with this cohort about how their data are being used is especially vital.

To reduce this skepticism among their constituents, higher education's leaders need to be steadfast in their commitment to and communication around privacy and security to ensure data are not shared, sold or used for any purposes other than those used to safeguard public health.

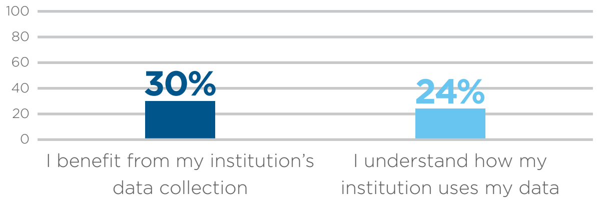
They should also seek to transparently communicate their commitment to privacy and ethical data usage at a higher level across the institution. The COVID-19 pandemic has created few new privacy concerns in the higher education landscape, but rather emphasized the need for urgency in responding to existing threats. Institutional leaders might consider undertaking a project to map out the "data life cycle" for contact tracing to ensure appropriate controls are in place before going live with an application or a third-party vendor.

Now is the time to ensure that institutional data privacy policies, processes and procedures are working the way they should and are reinforcing leading practices the industry has identified as effective. This can be accomplished by proactively outlining the processes and controls that are in place to safeguard student data. Some of these may include:

- Notice of consent
- Data classifications
- Third-party vendor evaluation
- Acceptable use policy
- Data-handling policy
- Privacy governance boards
- Risk assessment

Educating the Public About the Value of Contact Tracing and Data Collection

Another critical component required to ensure adoption of contact tracing on college campuses centers around student education. In EDUCAUSE's student survey, only about 30% of respondents agreed or strongly agreed that they benefit from their institution's collection and use of their personal data. And only about 24% agreed or strongly agreed that they understood how their data is used.



There are a number of ways that higher education leaders can start to bridge this gap.

- **Develop an institutional privacy governance board if one is not already in place at your institution.** During a crisis as unprecedented as the COVID-19 pandemic, there are bound to be multiple instances of unusual ethical questions and ambiguous circumstances that will require steadfast leadership, institutional agility and strategic thinking. With the goal of promoting a balance of perspectives from across the institution, formal privacy governance boards are essential to the ethical review and adjudication of complex information and data management matters. These committees are typically composed of a mix of knowledgeable faculty and administrators, while some integrate students as well. In combination with an institution's privacy office, these boards can help demystify student privacy and data protection concerns inherent in the daily operations of colleges and universities. Further, they can help shape new policies and procedures in response to emerging threats.

- **Use language that is accessible, accurate and tailored to the current environment.** For instance, research shows that “tracing” is a more palatable word than “tracking.” Beyond careful word choice, the language used in any educational materials should be as close to layperson’s terms as possible without losing the intended meaning.
- **Create a document that explains contract tracing — what it is, what it is not and how it will be used.** This resource should proactively answer frequently asked questions related to data security, use, storage and destruction. These guidelines will place a burden of responsibility on those working with vendors on the front end to ensure that any third parties can meet these standards in order to provide safety guarantees to students (encryption, limited access and other technology controls).
- **Tailor any technology to the end user.** For students, it is critical that any new technology be integrated seamlessly into their everyday lives and feel like the myriad other personalized applications they already use.
- **Develop privacy awareness training for students that can become part of their orientation.** Many institutions are already building this into their reentry plans for fall 2020 to ensure that students understand their rights and have the training required to make informed decisions about their data.
- **Clearly articulate the tangible benefits to students.** Consider, for instance, Snap Maps, a feature of Snapchat that allows users to track the location of their contacts. Part of the reason students may be willing to give up their privacy for this app is because it is immediately and tangibly beneficial to them to be able to find their friends. In the same way, leaders need to bring the advantages of contact tracing to life for students through storytelling that highlights the benefits of adherence to these measures and the risks of failure to comply.

As colleges and universities begin to reopen to students in the fall, contact tracing will play a vital role in the safety and security of everyone on campus. Yet, in order to ensure the efficacy of this disease control measure, student adoption is key. With growing skepticism about ethical data usage, especially among Generation Z, college and university leaders must work diligently to demonstrate a commitment to data privacy and security while educating their constituents about the benefits and risks of contact tracing.

Key Takeaways

To encourage the campuswide adoption of voluntary contact tracing measures, higher education leaders should:

Think differently.

Remember that contact tracing can only be effective with widespread student adoption, which is contingent upon trust.

Plan differently.

Integrate data security and privacy training into student orientation plans for the fall. Make it available on demand.

Act differently.

Communicate transparently with campus constituents (especially students) about how data collected via contact tracing will and will not be used.

HURON

huronconsultinggroup.com

20-0911