Digital Sanctuary: Protection and Refuge on the Web?

When I was growing up as a missionary kid, *sanctuary* was defined for me as a place of holiness and worship. It was where you weren't allowed to run or play. You would get dirty looks, or a disapproving *tsk-tsk*, for talking loudly or laughing. There were unwritten rules about how you dressed, how you behaved, and to whom you deferred. The sanctuary itself, the physical space, was designed to be grander than life. The sanctuaries I visited often had tall ceilings adorned with intimidating lighting fixtures; the pulpit was an ornate wood podium flanked by candelabras and throne-like chairs. The sanctuary was designed to inculcate a sense of reverence.

I've had a tempestuous relationship with the idea of sanctuary since rejecting my religious upbringing. But *sanctuary* is a term that keeps coming up as I think about the role of higher education in today's tumultuous social and political context. For me, it has started to mean "refuge" and "protection," drawing inspiration from the sanctuary movement that has seen a recent resurgence. It is with this definition that I want to respond to Michael Caulfield's question: "Can higher education save the web?"[1]

What responsibilities do universities and colleges have in providing sanctuary for student data and for students' digital footprints?

Sanctuary as a place of protection can be traced back to Greek and Roman societies, where churches sometimes harbored people who were under some form of persecution. In medieval Europe, a sanctuary knocker was a church's invitation for sanctuary seekers to signal their request for asylum. In recent times, sanctuary movements in the United States began in the 1980s as thousands of refugees fled civil wars in Central America. John Fife, a reverend at the Southside Presbyterian Church in Tucson, and his congregation provided food, shelter, and medical care to refugees and helped them apply for political asylum, as established by the U.S. Refugee Act of 1980 (Public Law 96-212). When most of the refugees were denied asylum despite meeting the legal criteria,[2] Fife amped up his support for refugees (including bringing refugees across the border), aided by John Corbett, a Quaker who was inspired by church/Christian efforts to help runaway slaves as part of the Underground Railroad in the 1840s and 1850s. The sanctuary movement of the 1980s did not end well for the sanctuary workers: Fife, Corbett, and nine others were arrested and charged with violating multiple federal laws (Corbett was acquitted; Fife was found guilty).[3]

The sanctuary movement has recently resurfaced in response to U.S. President Donald Trump's crackdown on undocumented immigration. As a result, some colleges and universities have declared themselves to be sanctuary campuses for undocumented students. Although the definition of a *sanctuary campus* varies, the declaration typically means that the campus will refuse to comply with requests to grant campus/student access to immigration enforcement officials. The legal ramifications of declaring a sanctuary campus are unclear, but the political statement that higher education institutions have a role to play in protecting students underlies the sanctuary campus designation.

Again, how does this all fit into questions about how higher education can save the web? For too long, universities and colleges have accepted the "terms of service" for how educational technology vendors handle student data. Caulfield noted: "As the financial model of the web formed around the twin pillars of advertising and monetization of personal data, things went awry."[4] This has created an environment that puts students at risk with every click, every login. It disproportionately affects the most vulnerable students: undocumented students, students of color, LGBTQ+ students, and students who live in or on the edges of poverty. These students are prime targets for *digital redlining*: the misuse of data to exclude or exploit groups of people based on specific characteristics in their data.[5] Thus, in higher education, we need to pay attention to the demands we place on students to produce data (e.g., application forms, SIS requests, learning management systems) and to how we care for that data (e.g., storage, transmission). Also, and perhaps most important in response to the influx of "learning-focused" technologies, we need to recognize and deconstruct our perspectives on the relationship of data to our understanding of student learning.

It's time to question assertions that the more data we have on students, the more we will understand their learning. Audrey Watters argues: "We have confused surveillance for care. . . . When you work for a company or an institution that collects or trades data, you're making it easy to surveil people and the stakes are high. They're always high for the most vulnerable. By collecting so much data, you're making it easy to discipline people. You're making it easy to control people. You're putting

New Horizons Editor: **Michael Caulfield**

By AMY COLLIER

people at risk. You're putting students at risk."[6] I have seen this in action: educators, technologists, designers, and administrators often are willing to trade student data for measurable signals of impact and can be terribly cavalier about the risks to students' physical and digital safety.

What responsibilities do universities and colleges have in providing sanctuary for student data and for students' digital footprints? How might higher education institutions resist the black box algorithms[7] into which they so freely feed student data? How might "digital" specialists and administrators reflect the caring, protective, and empathetic mindset of sanctuary movements? How might colleges and universities shape, rather than simply adopt, the ways that companies treat data?

We in higher education need to seriously consider how we think about and handle student data, and we need to respectfully and empathetically acknowledge where our practices may cause harm. I believe we must advance our institutions as "digital sanctuaries," and I have proposed an evolving set of seven strategies to do so.[8] Some of these strategies may be considered best practices in terms of data security, FERPA compliance, and IT operations, but some are not yet standard procedure.

1. *Audit student data repositories and policies associated with third-party providers.* Document every "place" that student data goes and what the policies are for handling student data. What third parties have access to student data, why do they have access, and what can they do with the data? Who decides—and how are decisions made—about third-party access to student data? Do students get a say?
2. *Have a standard and well-known policy about how to handle external inquiries for student data and information.* This is less about staff mishandling student data and more about the coercion and intimidation that could yield problematic results if there are no clear guidelines for staff to follow. Even if designated a digital sanctuary, a campus may be legally bound to release some student data, but it should have clear processes and requirements associated with those situations. Staff should understand how and when they can say no to inquiries about students, and campuses should investigate the legal limits of noncompliance with such inquiries.
3. *Provide an audit of data to students who want to know what data is kept on them, how the data is kept, where it is kept, and who else has access.* That is, if students want to know about their data, the institution should be able to give them that information. Better yet, students should be allowed to download every bit of their data so that they can parse it themselves. Consider giving students a chance to rap the sanctuary knocker to signal their desire for more data protections.
4. *Have clear guidelines and regulations for how data is communicated and transmitted between offices.* Campuses can better protect student data transmitted between the people and offices that should have access (e.g., by not transmitting data via email). Campuses should have clear policies and guidelines about the protection of student data on mobile devices.
5. *Take seriously the data policies of third-party vendors.* Don't work with vendors whose contracts stipulate that they can use and share student data without the consent of students or the institution.[9]
6. *Closely examine and rethink student-tracking protocols.* How necessary are learning dashboards? What are the risks of early-warning systems? How problematic are the acceptable use policies? How long does the institution need to keep data? Does it really need all of the data being collected?
7. *Give students technological agency in interacting with the institution.* Implementing a Domain of One's Own initiative, which puts students in the system administrator role for their domain, can be a way to give students more control and protection over their data. This may not be enough, however, since students could easily expose themselves to malicious and dangerous forces (e.g., hackers) through their own domains. A robust educational and mentoring program is also required. As a result, students can learn how to connect their data, via their domains, in ways that are safer and more manageable.

These ideas need to evolve—and I expect they will as we work together to flesh out, question, and develop the strategies. Let us, please, gather student data with more care. Let's use it with more care. Let's share it, save it, obfuscate it, or even delete it permanently with more care. And let's take on a leadership role in conversations about data. It's time for those of us in higher education to lead discussions about how best to provide digital sanctuary—protection and refuge—for students and their data. Who else but us? ■

Notes

1. Michael Caulfield, "Can Higher Education Save the Web?" *EDUCAUSE Review* 52, no. 1 (January/February 2017).
2. This still happens today. See Nicholas Kulish, "Torture Victim, Expecting a U.S. Handshake, Was Given Handcuffs Instead," *New York Times,* June 13, 2017.
3. For more about the origins of the sanctuary movement, see (and listen to) "Church (Sanctuary, Part 1)," episode 249, *99% Invisible,* February 28, 2017.
4. Caulfield, "Can Higher Education Save the Web?"
5. See Chris Gilliard, "Pedagogy and the Logic of Platforms," *EDUCAUSE Review* 52, no. 4 (July/August 2017).
6. Audrey Watters, "Ed-Tech in a Time of Trump," *Hack Education,* February 2, 2017.
7. Frank Pasquale's book *The Black Box Society: The Secret Algorithms That Control Money and Information* (2015) is a must-read.
8. Amy Collier, "'It Should Be Necessary to Start': Critical Digital Pedagogy in Troubled Political Times," *Red Pincushion,* March 3, 2017.
9. See "Privacy Evaluations" from Common Sense Media for some good resources.

Amy Collier (acollier@middlebury.edu) is Associate Provost for Digital Learning at Middlebury College.