the ethi{CS} project

How to Respond… When Students Tell You They Don't Care About Privacy

By Michelle Ciccone

Controversial issues around digital surveillance and online privacy make for engaging and unpredictable classroom conversation. Whether discussing the growing location tracking industry, or the use of cell-site simulators by some local law enforcement agencies, or even the ability for a loved one to direct the digital content you see, asking students to consider the ethical boundaries of digital data tracking is fodder for rich discussion.

But, in the midst of these classroom conversations, inevitably comes that comment. You know the one. We've all heard it: from friends, coworkers, family members.

"Well, I don't really care anyway. I'm not doing anything wrong so I have nothing to hide."

This comment can stop the discussion dead in its tracks. While it isn't helpful to sow the seeds of paranoia, the fact is that the apps we use, the companies that own them, the government agencies tasked with protecting us, and the hackers we never see really *are* watching what users do online, often in ways we don't remember opting in to. And it is imperative that all users, including our students, pay attention to this digital surveillance ecosystem.

So how might an educator respond when a student says they don't care about privacy? Below are three things to keep in mind.

First, understand that your students do in fact care about protecting their privacy. It just may not look how you expect it to. But young people do actively protect their private information in a variety of ways, including creating multiple social media accounts meant for different audiences and using defensive privacy practices such as the use of VPNs or ad blockers.

Begin classroom consideration of digital privacy by inviting students to reflect on their own digital privacy tactics. How do they decide who can have access to their public-facing profiles? What do they do to protect certain details about their preferences, movements, and activities? Sometimes young people recognize the actions they take as pro-privacy strategies, but sometimes they don't, and it takes someone else to help them distinguish between "just something I do" and an action taken to maintain privacy. By first helping students understand the actions they themselves already take in consideration of their own privacy, we can help students identify additional ways that privacy can be planned for and protected.

Second, move the conversation away from "why does it matter if this information is shared" to "why does this information need to be shared." When faced with the *"why should I*

care" line of argument, there can be a temptation to respond by upping the ante, asking students to consider increasingly egregious privacy violations. "You don't care about that? Well what about this?!" This attempt at "shock and awe" rarely works though.

A more productive line of inquiry moves away from challenging students to care, and instead asks students to consider why a given piece of digital information needs to be shared to begin with. Consider specific scenarios: does the video conferencing app Zoom need to send users' location and device information to Facebook in order to perform its stated function? (Zoom eventually removed the code that enabled this, so the answer was "no.") By depersonalizing the issue and flipping the focus from "why should I the user care" to "why should they the company have access to that," the burden of proof falls on the organization collecting the information, not on the individual student to defend their right to keep a certain piece of information private.

Third, highlight instances of a technology (and its use) being altered in response to privacy concerns. Calling attention to these changes reminds students that technologies are not inevitable in their design and implementation, and that prioritizing privacy can in fact drive innovations. This is, of course, particularly useful in the computer science classroom, as we train the next generation of technology developers.

Examples abound, including the Zoom case above. Tracing shifts in laws that regulate technologies can also be instructive. For example, recent municipal bans on the use of facial recognition software by city agencies have been spearheaded by lawyers, researchers, and activists who understand that encoded bias makes facial recognition software highly inaccurate when used on the faces of people of color. It is important to demonstrate to students that default technology uses and associated privacy practices that may feel innocuous to some may actually be harming someone else. But it is equally important to empower students to demand, and even design, alternative futures.

The most effective way to respond to *"why should I care about my privacy online?"* is to reframe the conversation from the get-go, and the points above can help. But we can also demonstrate what being privacy-minded looks like in big and small ways. **Think about your own classroom routines and consider: do these practices instill the pro-privacy stance you hope to see in your students?** For example, when introducing a new app or educational website for student use, do you engage in conversation around what the Terms of Service allow for, or how this new tool integrates and shares data with other platforms? If we want our students to value privacy, then we must demonstrate what this looks like everyday.

Michelle Ciccone is a Technology Integration Specialist at Foxborough High School and a Research Affiliate at the Tang Institute at Phillips Academy.