In a post-9/11 world dominated by digital technology it is very important that undergraduate students be exposed to different perspectives on the effects of information on their lives. Whether the issue is the security of digital data, the privacy implications of information infrastructures or the proliferation of voyeurism by both individuals and the state, most young people have explored the implications of the information environments that they navigate. While university classrooms are a perfect venue for the discussion and development of these issues, it can be difficult to bring them into a classroom environment. In many cases the topics to be discussed are controversial and require teachers to examine subjects that can involve proscribed behaviors like computer hacking or politically and emotionally charged subjects like sexuality, religious belief and racism. To explore these information topics requires planning and vigilance in the classroom in order to impart knowledge and teach critical thinking skills while avoiding encouraging unethical behavior or offending individual students.

My experience grappling with these challenges has occurred over five years of teaching undergraduates about information security, privacy and surveillance. I find in my courses that I must continually balance classroom sensitivities with encouraging students to consider different ways of thinking about their informational lives. My lectures and demonstrations have covered topics ranging from how to crack computer passwords and scan networks for software vulnerabilities to racial profiling and the proliferation of amateur pornography. My students are conservative, liberal and libertarian. They may be deeply religious and ambivalently agnostic in equal measure. Some are quite outspoken while others rarely say a word over an entire semester. In short, they are typical of most undergraduate student bodies, and I have to strive to keep everyone interested while not offending terribly or crossing ethical or policy boundaries.

The course material I teach covers several topics, including cybercrime, identity theft, surveillance practices and voyeurism. Most of the class discussions include considering the role that technology plays in all of these activities. In all the cases the material can be controversial. It is difficult to lecture on computer security without exposing students to tools and techniques that they could use to teach themselves how to hack others’ information systems. Teaching about surveillance or voyeurism in society means students must confront differing ideas on race, privacy and what is considered offensive or illegal.

Research exists on the teaching of controversial subjects ([1], [2], [3]) and there are a variety of materials available to help educators in their efforts. But nothing quite prepares you for that moment when 30 young people freeze, everyone realizing that a potential landmine has been triggered and all looking to you as the professor to defuse the situation. At the best of times this instant is the ultimate teaching moment, where the class moves beyond the readings and lecture into a more visceral understanding of the subject material. At the worst of times it becomes an effort to defuse a bomb before it causes potentially serious damage to classroom cohesion and student morale (and possibly one’s career). One response is to simply avoid truly controversial subject material in favor of safer ground. But this path, at least for me, leads away from those breakthrough moments that keep me coming back semester after semester to fresh rooms of young faces. And by coming back again and
again, I have identified several distinct challenges to teaching controversial subjects, as well as solutions that I have used with some success to overcome pedagogical barriers presented by the subject matter.

Challenges

I usually face four primary challenges in my courses, depending on whether I am teaching about security or surveillance. First, the subject matter requires direct experience on the part of the students. You cannot learn about scanning networks for vulnerabilities by just reading an assigned text, nor can you discuss the proliferation of surveillance technology without some experience of that growth. I must find a way to provide my students with opportunities for empirical exploration of the topics we cover. The second challenge often directly conflicts with the first: some of the practices and technologies cannot be used in a university or classroom setting. This barrier is particularly true in computer security where running security and hacking tools against the university network is dangerous and forbidden. In these cases I have to find ways to emulate these tools to provide the experience in a safe and legal environment. My third challenge is that topics are often politically sensitive. The risk here is that classroom discussions can often devolve into political discussions that are off-topic and detract from the real point of the lecture. This digression often happens when discussing surveillance practices from the point of the new capabilities afforded by technology. The risk is that students focus too much on the ideology of surveillance and want to gloss over the infrastructures of surveillance that could provide them with more insight into their ideological positions. A fourth challenge I have had is that classroom materials are often technically complex or visually graphic. It is a challenge to keep student interest when they are exposed to technical information that they may not understand, even when they are very interested in the high-level ramifications of that technology. And discussions about sexuality and violence in media are among the most difficult to have as the risk of negative reactions by students is always present.

Approaches

To meet the challenges of teaching these controversial topics, I have benefitted from several techniques developed out of my teaching experience. In each case the goal of the technique is to maximize student involvement with the material so that each student must contextualize the subject material within his or her own daily lives and practices. This allows a student to engage the topic by situating it within their own comfort zone, while also providing a ready feedback mechanism to me as they discuss the topic in class and in their assignments.

The first technique that I employ to overcome controversy is a heavy reliance on pop cultural references to classroom material, particularly in film and music. My syllabus includes several movies shown over the course of a semester that explore relevant themes and that I use to anchor papers and classroom discussions. Movies such as Primer, GATTACA and even Live Free or Die Hard provide a less threatening entry into issues of emergent complexity, genetic discrimination and critical infrastructure threats, to name a few examples, than a more direct approach. Students are required to combine the films with more challenging readings and lectures, and assignments encourage a synthesis of both. I have used music in the same way, particularly in the area of surveillance, by having students submit songs with themes of watching or voyeurism to an online class playlist. In both cases the familiarity of pop culture provides a bridge to the class material while also proving entertaining and motivating students to participate.

A second technique that I use involves the construction of hands-on exercises in security and surveillance that allow students to explore these themes empirically, but in a relatively safe and controlled way. Internet technology greatly enhances our capabilities to provide students with these experiences, allowing students to explore at their convenience and eliminating the need to undertake activities in class that might violate university policies. A good example is the demonstration of scanning tools used by security professionals as well as hackers to enumerate vulnerabilities on networked computers. Most universities have strict prohibitions against running these tools, for obvious reasons. But there are many websites, usually those of security companies, that will run versions of these tools against the personal computer of anyone visiting their site. The purpose of these exercises is to warn consumers about potential security problems with their machines (and to market products to them as a result). The scans are legal and benign, but
they demonstrate the technologies I discuss in lectures. For non-technical students this exercise provides hands-on experience with a tool they might otherwise not fully understand.

To teach surveillance I rely on similar exercises, but with a slightly different focus. A primary surveillance assignment in my courses involves the students spending several weeks looking for and documenting surveillance cameras that they observe in their daily activities. These cameras are noted, along with location and the time they were observed, and the students submit lists of cameras over the course of the assignment. All observed cameras are then posted to a customized online map, creating a mashup of locations that represent all the cameras found by the class. The result is a dramatic visual effect as we explore the map in class and observe just how saturated the geography of our lives is with surveillance technologies. Most of my students respond to this assignment by telling me that they become much more aware of the presence of camera surveillance in their daily lives. This internalized awareness of surveillance in their personal environment tends to exceed anything that could be achieved on the basis of classroom readings and lectures alone.

A third technique I use to avoid letting controversial subject matter negatively impact class discussions is to designate a “safeword” for the class. I use this mechanism when the topics covered in classroom discussion have a better than average potential for making students uncomfortable or when strong positions on race, religion, politics or sexuality are likely to occur. In these situations the class agrees beforehand that all arguments and discussions are allowed so long as students are polite and respectful. If anyone in the class (including myself) feels that the discussion is moving into an area that makes them uncomfortable they may use the safeword and bring an immediate pause to the discussion. Invoking the safeword requires the class, facilitated by me, to reset the conversation in a way that either addresses the issue that provoked the use of the word or to move on to another topic of discussion. The safeword is usually something amusing and benign – in my classes the word “cupcake” has been the most commonly selected trigger word. I have seen the word used several times, usually to stop arguments that were beginning to grow heated or where very emotional arguments around religion or ethnicity were beginning to be articulated.

The safeword concept has been quite useful because students often find it humorous, resulting more often than not in the class being amused by its use rather than offended by the situation that it was used to defuse. I also find the safeword trope benefits the overall class interactions by giving every student an easy way to communicate about choice in these situations. Even reserved students who do not feel comfortable contributing to classroom discussions or confronting others with their opinions can, by simply saying a word, affect and direct the entire discussion. Saying the safeword requires no explanation of why the student chose to use it, but rather imposes on me an immediate responsibility to adjust the discussion with no questions asked.

Working with undergraduates to interrogate some of the less utopian aspects of information technology is both difficult and rewarding. Many of my students come to my classes understanding little about subjects like cryptography, privacy or social sorting. At the same time they often have emotionally charged opinions about the roles that these and other aspects of security and surveillance play in their lives. Digging deeply into the subjects can be uncomfortable for them and for me, but by attempting to provide empirical experience of the material and empowering students to engage classroom material on their own terms and within their own limits has proven a successful pedagogical strategy.

Resources Mentioned in the Article

