

Jimmy Benjamin

PHIL 355E

Professor Matthew Montoya

08/19/2026

Reflection

This summer I took the PHIL 355E ethics course for cybersecurity, engaging with tools ranging from utilitarianism, kantianism, virtue ethics, and Ruism to incorporate their principles into case analyses. Aside from these ethical tools, the topics learned in this course all shared the core focuses of maintaining safety and awareness of technology conflicts for everyone. They not only described the harm being inflicted from an ethical view, but the combined use of the tools and texts elaborated the consequences to aid clearer analysis. To conclude this semester, I am reflecting back on the topics of *privacy*, *whistleblowing*, and *cyberconflict* to show how my views have shifted and leaving a key takeaway for each.

Privacy was the very first topic where we looked at why everyone, including hacktivist groups, deserves it regardless of being used to commit immoral acts. Before this class, I always thought hackers never deserved their own privacy, due to the damages caused by using it against their victims. After a Case Study about the Ashley Madison (dating app) breach, I considered how the majority of hackers are people living their own lives as well, and how *they* would react with the same panic of having *their* lives invaded. The intention was to catch people cheating on their partners, done by the Impact Team hacking group in response to the app charging a fee to permanently delete accounts. They also threatened to expose profiles and records just to expose

cheaters. Now I'm not saying all hackers are moral, some are and some aren't, but the wrongs and motives don't matter if everyone, hackers included, wasn't allowed to live freely by themselves. In short, we would all feel equally violated from living so publicly, and privacy is valuable in protecting our advantage to keep us knowing ourselves best.

Second topic, whistleblowing is the act of an insider who exposes illegal, or hidden, information within an organization to others. One example is Edward Snowden's act of exposing NSA's secret conducted surveillance to the public, leaking bulk telephone metadata collection and granting access to personal emails, search histories, and confidential data from using secret court orders and programs. Snowden stated that no one should have to live in a world where the government controls privacy, reiterating the cruciality of attaining privacy once again. In terms of my thoughts on this, they are pretty much the same in the sense that whistleblowing is the challenging means of risking yourself to protect the public from great harm. However I will admit that I didn't really know too much about reported incidents, but I've found that those who have committed the crime acted so on the basis of care ethics. Care ethics being the moral theory of empathy and maintaining relationships, acting on obligation to show compassion to each other, but care does *not* equate to doing the right duty. I see whistleblowing as a winning game, because you once again put everyone else first by exposing illegal data, even though violations made are based solely on righteous care *and* duty rather than self-satisfaction.

Last, but certainly not least, the topic of cyberconflict. Cyberconflicts are the hostile acts of utilizing computer systems and networks to damage, or spy, upon major infrastructures for the ends of personal benefit from political, economic, or strategic gain. Some notable cases include

the Stuxnet worm, created by Israel that infected Iranian industrial site machines by hunting program software, and the Stryker attack, the largest medical technology corporation whose internal system was compromised by the Handala (Iran) hacktivist group. Stuxnet was declared as the first ever successful cyberweapon, but both of these shared the goal of political gain and targeting infrastructure as stated in the start. I agree cyberconflicts are of course ethically unjustifiable, but I do think they *could* be justified from a consequentialist view. There were no casualties among the two, but international and defense laws *should always* be considered to safely prevent further escalation. To wrap up this reflection, ethics in cybersecurity shows how technology resonates with our own lives by practicing privacy, care, and awareness of issues to maintain online safety no matter the arising wrongs.