

Cybersecurity is not only a technical domain but a deeply ethical one. As our world becomes increasingly interconnected, our digital decisions have profound consequences. This cybersecurity ethics course has challenged me to rethink assumptions, utilize philosophical frameworks, and consider the ethical implications of building, using, and regulating technology. In this reflection, I will examine three key areas where my understanding has significantly shifted: the shared responsibility of maintaining cybersecurity, the evolving ethical value of privacy, and the moral complexity of cybersecurity at scale. These ideas have reshaped how I understand the intersection between ethics, power, and responsibility in the digital age.

Early in the course, I saw cybersecurity as something that fell mostly on professionals in IT departments, system administrators, or government agencies. I now realize that cybersecurity is a deeply shared responsibility. Individuals can make careless choices (like using weak passwords or clicking malicious links). Still, the systems they're navigating encourage risky behavior through poor design, confusing language, or an overwhelming number of decisions. At the same time, corporations often fail to invest in secure infrastructure, delay patches, or prioritize profit over user safety.

This shift in thinking has been shaped by deontological ethics, which emphasize duty and moral obligation. From this perspective, both individuals and institutions have ethical duties in the digital space: individuals should strive to act responsibly, and corporations must uphold their duty to protect users from preventable harm. Utilitarianism further deepens this point, highlighting that small design choices (such as forcing 2FA or eliminating dark patterns) can generate large-scale benefits for users. System design and user behavior must work in ethical harmony to protect everyone.

Before this course, I saw privacy as something similar to personal preference; privacy is something people could give up in exchange for convenience or free services. I now understand that privacy is a moral right closely tied to human dignity, autonomy, and freedom. Once data is collected, it can be repurposed in ways that individuals never consented to, often without transparency or accountability. Exploring this issue through rights-based ethics, such as deontology, Confucianism, and contractarianism, I came to view privacy as not optional but essential. Data collection without meaningful consent violates personal autonomy, while surveillance at scale creates a chilling effect on free speech and self-expression. In some cases, these frameworks also allow us to assess the ethical character of corporate entities. What does it say about a company if it prioritizes collection and tracking over honesty and respect? Privacy is a foundational principle to ethical digital life that the digital ecosystem must protect.

Finally, I initially viewed cybersecurity as localized technical problems. However, this course has helped me see how cybersecurity operates on a national and global scale, involving international actors, complex infrastructure, and geopolitical consequences. The ethical stakes of cybersecurity don't stop at borders. Cyberwarfare, global malware outbreaks, and state-sponsored surveillance have exposed how cybersecurity decisions have cascading effects across communities. Ethical tools like utilitarianism can help assess global risks and benefits. However, applying ideas like the veil of ignorance is important when designing systems to ensure everyone, particularly the least privileged, benefits. We should apply relational responsibility, compassion, and attention to marginalized or under-resourced populations. Cybersecurity at scale requires ethical foresight and humility. Solutions must consider what's possible, what's just, and who is most affected.

Ultimately, this course has shown me that ethical thinking is essential to cybersecurity. No matter how simple, every decision we make has some moral weight. My thinking has shifted from seeing cybersecurity as a technical checklist to viewing it as an ethical ecosystem where responsibility is shared, privacy is protected, and decisions made at scale ripple across the world. As I move forward, I want to carry with me the reminder that cybersecurity isn't just about what can be done, but what should be done. Ethical choices in digital spaces have real, human consequences.