Task 1: Review the Situations

Video 1: YouTube Link 1

- **(a) Was Alice's act illegal? Why or why not?**
  Yes, Alice's act was illegal. When Alice modified the URL to input her roommate's student ID and accessed her roommate's transcript without authorization, she violated the Computer Fraud and Abuse Act (CFAA). This law prohibits intentionally accessing a computer system without authorization or exceeding authorized access. Even though Alice did not cause harm or steal information, unauthorized viewing of private academic records is enough to constitute a violation under the law.

- **(b) Was Alice's act unethical? Explain.**
  Yes, Alice's act was unethical. Ethics requires respecting the privacy and confidentiality of others' personal information. Even if Alice was simply curious and did not misuse the information she accessed, intentionally viewing someone else's academic records without consent shows a clear disregard for privacy and trust. Ethical standards in computing and academic environments emphasize respecting others' rights to data confidentiality.

Video 2: YouTube Link 2

- **(a) Was Alice's act illegal? Why or why not?**
  Alice's actions could potentially be illegal. Although she was instructed by her boss to collect information, her collection of highly sensitive personal data — including cached web traffic, personal email contents, and private documents — may have violated privacy protection laws such as the Electronic Communications Privacy Act (ECPA). Gathering information that goes beyond work-related files, especially personal communications, often requires a warrant or legal authorization that Alice did not have.

- **(b) Was Alice's act unethical? Explain.**
  Yes, Alice's act was unethical. Ethical behavior requires respecting the boundaries of privacy, even during internal investigations. Although she was asked to gather all information, Alice overstepped by accessing personal browsing history, social media, and personal email without consent. Instead of limiting her search to professional data, she intruded into Charlie's personal life, violating fundamental principles of privacy and respect.

- **(c) Were Charlie's rights violated? Explain.**
  Yes, Charlie's rights were violated. Employees, even when using employer-owned equipment, maintain some expectation of privacy regarding personal communications and activities. By

accessing private, non-work-related data without Charlie's knowledge or a legal warrant, Alice infringed upon Charlie's rights to privacy and confidentiality. Turning over this personal information to law enforcement without proper legal procedures further compounded the violation.

Task 2: Ethical Hacking

1. One place where Arizona law is more stringent:

In Arizona, under A.R.S. §13-2316, unauthorized access to a computer, computer system, or network is considered a **Class 6 Felony**, even if no data is changed, stolen, or damaged. The law criminalizes simply gaining access without permission, emphasizing the importance of protecting digital systems against any form of intrusion. Arizona does not require proof of intent to harm, steal, or cause damage; unauthorized access alone is enough to be charged. This is stricter compared to some states that require evidence of damage or malicious intent.

2. One place where Georgia law is more stringent:

In Georgia, under O.C.G.A. §16-9-93, not only is unauthorized access prohibited, but the law also explicitly allows **civil lawsuits** against offenders by victims of hacking or data theft. Georgia's statute is stricter in the sense that it gives immediate remedies to victims, allowing them to recover financial damages without waiting for criminal prosecution. This provides stronger, more direct protection for individuals and organizations who suffer harm from cyber intrusions.

3. Your overall assessment of which law is stricter and why:

Overall, **Arizona's law is stricter** because it criminalizes unauthorized access itself, regardless of whether harm occurs. In Georgia, the harshest penalties often require proof of data theft, financial damage, or malicious activity. Arizona's approach sends a stronger deterrent message by treating even minimal unauthorized access as a serious crime (felony), aiming to prevent digital crimes at the earliest stage.

4. Your opinion of which law is better and why:

I believe **Georgia's law is better** because it provides a more balanced approach to cybersecurity enforcement. By focusing penalties primarily on cases involving actual harm, data theft, or financial loss, Georgia's law recognizes the difference between malicious hacking and minor or accidental access. Additionally, offering civil remedies to victims allows quicker resolution and compensation compared to relying solely on criminal courts. This combination protects both cybersecurity and fairness more effectively.