Name (print): STUDENT NAME

- INTEGRITY: By taking this exam, you pledge that this is your work and you have neither given nor received inappropriate help during the taking of this exam in compliance with the Academic Honor Code of Georgia Tech. Do NOT sign nor take this exam if you do not agree with the honor code.
- DEVICES: If your cell phone, pager, PDA, beeper, iPod, or similar item goes off during the exam, you will lose 10 points on this exam. Turn all such devices off and put them away now. You cannot have them on your desk.
- ACADEMIC MISCONDUCT: Academic misconduct will not be tolerated. You are to uphold the honor and integrity bestowed upon you by the Georgia Institute of Technology. Violations will be referred to the Office of Student Integrity.
  - Keep your eyes on your own paper.
  - Do your best to prevent anyone else from seeing your work.
  - Do NOT communicate with anyone other than a proctor for ANY reason in ANY language in ANY manner.
  - Do NOT share ANYTHING during the exam. (This includes no sharing of pencils, paper, erasers).
  - Follow directions given by the proctor(s).
  - Stop all writing when told to stop. Failure to stop writing on this exam when told to do so is academic misconduct.
  - Do not use notes, books, calculators, etc during the exam.
- TIME: Don't get bogged down by any one question. Note that this exam has 100 total points. You should use the number of points on a problem as the approximate time you should spend on it. This exam has 13 questions on 15 pages including the title page. Please check to make sure all pages are included. You will have 1 hour and 45 minutes to complete this exam.

I commit to uphold the ideals of honor and integrity by refusing to betray the trust bestowed upon me as a member of the Georgia Tech community. I have also read and understand the requirements outlined above.

Signature: _____

Question	Points	Score
1	12	
2	6	
3	9	
4	6	
5	4	
6	6	
7	4	
8	6	
9	6	
10	8	
11	8	
12	10	
13	15	
Total:	100	

1. *(12 points)*

Multiple Choice. Circle the correct answer for each question.

(a) [1 pt] "Informational privacy" refers to

A. Freedom from physical intrusion

B. Freedom from interference in one's personal affairs

C. One's ability to change their personal information

D. Concerns affecting access to and control of personal information

(b) [1 pt] Which is NOT one of the four different characteristics a moral system should have?

A. Public

B. Rational

C. Informal enforcement

D. Legal

E. Impartial

(c) [1 pt] Which is a consequentialist ethical framework?

A. Deontological framework

B. Rights-based framework

C. Utilitarian framework

D. None of the above

(d) [1 pt] What is the textbook definition for cyberethics?

A. Ethical issues regarding the flow of information that is either enhanced or restricted by the flow of computer technology.

B. Evaluates the social policies and laws that have been framed in response to issues generated by the development and use of cyber technologies.

C. Ethical issues associated with computing machines and computing professionals.

D. Concerns networked information and computer communication devices and systems.

(e) [1 pt] In Chapter 2 of the textbook, the author identifies 4 common forms of ethical discussion stoppers, which of the following was not one of the discussion stoppers mentioned?

A. Morality is a personal and private decision

B. Morality is universal we all believe in it so why bother discussing it

C. It's wrong for me to judge another person or to impose my beliefs on them

D. Morality is a cultural or religious system of belief

(f) [1 pt] Under which type of ethical theory does act-deontology belong?

A. Duty-based

B. Contract-based

C. Character-based

D. Consequence-based

(g) [1 pt] Existing privacy laws do little to protect people from data mining because they do not cover:

A. Electronic records in the database.

B. Personal information that is implicit in the data.

C. Data exchanged between or across databases.

D. Data which is confidential in nature (medical, financial, academic)

(h) [1 pt] In the article "Hacking the Hill," hackers infiltrated a number of computers and networks in the US House of Representatives. This instance of hacking can be considered an act of:

A. Information Warfare

B. Cyberterrorism

C. Hacktivism

D. Activism

(i) [1 pt] In the article, "Heartland Payment System Data Breach," several cybersecurity breaches were mentioned. Which of the following breaches was the **original** breach which lead to the data loss?

A. Personnel Breach

B. System Breach

C. Network Breach

D. Cash register transaction

(j) [1 pt] In the video on the TJX data breach, hackers were able to infiltrate TJX's computer for over a year and a half and steal over 100 million credit cards and hit 2400 stores. Besides the amount of money lost, what made this story newsworthy?

A. TJX collected too much information

B. TJX kept the information too long

C. TJX didn't store data according to appropriate security standards

D. TJX did not have proper wireless network security

(k) [1 pt] A public revelation of private information meant to call attention to negligence, abuses, or dangers that threaten public interest is called:

A. Public Dissent
B. Justifiable Gossip
C. Whistle Blowing
D. Gross Treason

(l) [1 pt] An ethical issue that applies to personal relationships between individual professionals and other individuals such as clients is a:

A. Microethical issue
B. Macroethical issue
C. Accountability issue
D. Value Sensitive Design issue

2. *(6 points)*

True/False. Write the word "True" or "False" to indicate your answer.

(a) [1 pt] Data mining is not not considered an invasion of privacy because it is not personal data that resides in a database rather it is new facts, relationships, or associations about a person.

(a) **True, Ch. 5**

(b) [1 pt] The standard form of an argument is to list the premises first and then the conclusion.

(b) **True (Section 3.1.2)**

(c) [1 pt] An argument does not qualify as a strong argument if its premises are weak, even if it has a premise and a conclusion that is convincing.

(c) **False (p77)**

(d) [1 pt] In a *naturally private* situation, privacy can be lost but not violated.

(d) **True (p137)**

(e) [1 pt] According to Bernard Gert, morality is a system whose purpose is to prevent harm and evil.

(e) **True**

(f) [1 pt] A computer scientist is considered a professional like a civil engineer, doctor, or lawyer.

(f) **False**

3. *(9 points)*

Matching: Match each logical fallacy to its definition. Choose the **best** definition for each fallacy.

Types of Fallacies:

(a) [1 pt] Ad Hominem

(a) **6**

(b) [1 pt] Slippery Slope

(b) **9**

(c) [1 pt] Appeal to Authority

(c) **3**

(d) [1 pt] Appeal to the people

(d) **8**

(e) [1 pt] False Cause

(e) **2**

(f) [1 pt] Begging the Question

(f) **5**

(g) [1 pt] Division

(g) **4**

(h) [1 pt] Many/Any

(h) **1**

(i) [1 pt] Virtuality

(i) **7**

Descriptions

1. Many items of a certain kind, A, have property B. Therefore, any item of the kind A has B.
2. Argument that reasons that since X proceeds Y, X is the cause of Y
3. Appeal to the notion that anything an expert says is correct
4. Infers that the same attributes or characteristics that apply to the whole group must also apply to every part of the whole or every member of the group.
5. An argument whose premise(s) presume the truth of the conclusion
6. An argument that attacks a person rather than the substance of their argument
7. Claims that because something happens in a "virtual space" it has no impact on the real world.
8. X is popular. Therefore, X must be an acceptable standard.
9. X could possibly be abused; therefore, we should not allow X

4. *(6 points)*
Short answers: your answers to these questions should be no more than 1-3 sentences.

(a) [2 pts] What is the key difference between a virus and a worm?

Solution: A worm replicates on it's own, and does not require human intervention.

(b) [2 pts] What is the difference between hacktivism and cyberterrorism?

Solution: Hacktivism involves: civil disobedience, no damage to person or property, non-violent, not for profit, ethical motivation, willingness of culprit to accept responsibility.
Cyberterrorism involves: intention to cause harm to other people or systems.

(c) [2 pts] Give an argument why Active Defense, or "Hacking Back," is not morally justified.

Solution: You don't know for sure who you are targeting. Difficult to identify the true perpetrators. Most likely will be illegal, and breaking the law is wrong. You should not engage in "wrong" behaviors just because somebody else has.

5. *(4 points)*
Describe a scenario where breaking into a computer could be ethically justified. Under what ethical framework would this scenario be considered ethical and why?

Solution: Breaking into a computer to retrieve needed digital medical data to save somebody's life because the authorized user can not be found. Act-util.

6. *(6 points)*
In your textbook, there is a distinction made between "true" cybercrime and crimes which are assisted or exacerbated by cybertechnology. Name the three types of "true" cybercrime and give a brief example of each.

Solution: Piracy - Reproduce/Distribute copies of proprietary information
Trespass - Unauthorized access to system/site
Vandalism -Disrupt access, Destroy/Corrupt data, damage systems

7. *(4 points)*
Consider the following argument:
Premise 1: Seventy-five percent of people who own Macs also own a iPod.
Premise 2: My roommate currently owns a Mac.
Conclusion: My roommate also owns an iPod.

(a) [2 pts] Is this argument valid? If it is not, what logical fallacy does it make?

Solution: not Valid, The Many/Any fallacy

(b) [2 pts] Is this argument strong or weak? (Justify your answer)

Solution: Not valid, but inductive and strong because the statement "my roommate also owns an iPod" is very likely to be true when we assume the truth of both premises. Pg 87

8. *(6 points)*
Define Data, System, and Network security and provide an example of each.

Solution: See page 176 in textbook.
Data Security - Concerned with vulnerabilities pertaining to unauthorized access s to data. Ex: Data is left on a flashdrive in a public place and is picked up.

System Security - Concerned with vulnerabilities to to system resources such as computer hardware, OS, and applications software. EX: Using liquid nitrogen to cool RAM in a stolen laptop in suspend mode so that you can remove the RAM, put it into a reader, and search for HD encryption keys.

Network Security - Concerned with securing computer networks from attacks. EX: DDoS attack against Comcast servers that bring down the entire network so nobody could get on the Internet.

9. *(6 points)*
As discussed in class, Richard Epstein believes that security can be viewed in terms of three key elements. Without all three you lack security. Name them and give a brief definition for each.

Solution: Confidentiality - Bad people can't see your stuff.
Integrity - Bad people can't change your stuff (at least without you knowing about it, and preferably not at all)
Accessibility - No matter what bad people do, you can still get access to your stuff. (Think DDOS attacks...)

10. *(8 points)*
The introduction of "cybertechnology" has had four major impacts on privacy. What are these impacts, and give an example of how each has affected privacy.

Solution: -Amount of personal information that can be gathered, indexed, and processed has increased.
-Speed - Personal information can be transmitted/looked up instantly.
-Duration of storage has increased (easier to retain more information)
-Kind of information has increased (every store purchase easily tracked with barcodes, etc)

11. *(8 points)*
List and describe at least **four** of the six tenants of "Hacker Ethics" as described by Steven Levy.

Solution: (4 of the following):
1. Access to computers should be unlimited and total.
2. Information should be free.
3. Mistrust authority-promote decentralization.
4. Hackers should be judged by their hacking (merit) not by degrees, race, age, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

12. *(10 points)*
Consider the following scenario:
You have been asked to observe how data-entry clerks use new accounting software at a large accounting firm. As part of an observational study, the clerks are informed that they will remain anonymous. You install logging software on several clerks' computers, and your analysis of these logfiles reveals that many of the clerks are making a particular data entry error when using the new software. These errors will cause the firm to lose money, and company policy clearly dictates that workers salaries will be docked for mistakes leading to loss of company profit. You report the problem with the new software package to your boss. Your boss demands that you turn over your log files so the company can follow-up with more training for the employees and ensure that the company is reimbursed for the errors from the employees' pay.

(a) [5 pts] Identify an ethical framework and use it to argue why you **should NOT** turn over the logfiles to your boss.

Solution: Virtue Ethics: Prime tenants of most virtue systems are "do not lie" and "keep your word". In this case, you promised to keep the clerk's data anonymous for the study, so you must do so. Contract Theory : You have an explicit contract (informed consent agreement) with the employees not to release their data in a non-aggregate data. Act Utilitarian: No, many people (the clerks) will lose happiness and only one (the boss) will gain a little happiness.
Duty Based (Kantian): If you expose the clerks, you are aiding an "end" (the company being reimbursed) by using the clerks as a "means". General rule is to never do this.
Social-Contract: The company didn't provide the correct training, so the clerks should not be held responsible.
Contract Based: The employees signed an employment agreement where they knew they would be docked for mistakes.
Rule-utilitarianism: Assuming the company runs more efficiently when blame is properly allocated, you should NOT turn over the log files. If many of the clerks are making the same error, it is unlikely to be all their fault. Therefore, the right thing to do is to ensure the blame is NOT placed on them, thereby preventing the real culprit (lack of training?) from avoiding blame. This would ensure the company provided the needed training and prospered, allowing all employees to retain their jobs and shareholders to prosper.
Rule-Utilitarianism: If you keep applying the rule "don't turn them in" the company could lose lots of money, go bankrupt, and everybody would lose their jobs.

(b) [5 pts] Identify an ethical framework and use it to argue why you **should** turn over the logfiles to your boss.

Solution: Contract Theory: You have an explicit or implicit employment contract with your company that states you should do what your boss says.
Act Utilitarianism: Turn over the names of a few employees so that the company and investors are not harmed by their lack of training. Help the many by hurting a few employees.
Rule-Deontological: Actions of employees that could be potentially detrimental to fellow employees and the company itself can not be excused or ignored.
Act-Deontological: In this situation (act) you must choose between two conflicting duties. You have a duty to the clerks to keep your word and preserve their anonymity. You also have a duty to your boss/employer and company to discharge your duties to them (for which you are paid). Because you agreed to your duties to your employer (were hired) before you did the study, and are doing the study in service to your employer, you should honor the company policy (which you presumably also agreed with when you were hired) that employees are docked pay for their mistakes.

13. *(15 points)*
According to Richard De George, the three conditions that must be satisfied before an engineer is morally permitted to "blow the whistle" are:

1.

2.

3.

In addition, if the following two conditions are satisfied, the engineer is morally **required** to "blow the whistle":

4.

5.

Army Specialist Bradley Manning is being detained on suspicion of passing a secret video of a US Army helicopter gunning down civilians in Iraq to the whistle-blower website WikiLeaks. With respect to **only** the leak of this video, which of the above conditions were met? And which were not? For each condition, explain why or why not. If you feel there is not enough information to make a determination, state what other information you would need to make a decision.

- Condition 1:

- Condition 2:

- Condition 3:

- Condition 4:

- Condition 5:

Solution: Allowed: (2pt each)
1. Potential for serious and considerable harm to the public good.
2. Engineer has reported the serious threat to their supervisor.
3. The engineers have exhausted the internal procedures for going over their superiors head if they do not receive support.
Obligated: (2pt each)
4. Have accessible, documented evidence that would convince a reasonable person that their opinion (about the potential for harm) is correct. 5. Have good reason to believe that by going public they will be able to enact change to reduce/eliminate the harm.

In the case of Army Specialist Bradly Manning: (1 point each) 1. Yes - Actions of military personnel could incite violence against American civilians, or harm innocents.

2. Unknown/No - News stories haven't said that he went to his boss, we suspect he did not, as nobody knew who the leak was until he told Lamo it was him.

3. Unknown/No - We don't know if he want up the chain of command, but he probably didn't.

4. Yes, he had the evidence (video)! No - He had not seen the video himself (it was encrypted, and wikileaks had to brute force the password before it could be viewed)

5. Yes - A change in public opinion towards the military's actions could force a change in its behavior. No - The public may not care about the video and no changes would occur.