CYBERCRIME

FINAL EXAMINATION

Course Number CR0014LEC
Spring 2004

Adjunct Professor Ronald N. Weikers

INSTRUCTIONS

Read the question and think about your answer, or outline it on scratch paper, for ten (10) minutes before you begin to write your answer. If you wish, you may use outline form for your answer, as long as it is organized, comprehensive and comprehensible.

You may consult your own books, notes and charts, but you may not use a computer or any other electronic device. Your answer must be neatly handwritten in bluebooks or on pre-printed charts using an ink pen.

Cite abbreviated statute names and section/subsection numbers, shortened case names, and abbreviated names of parties.

You are solely responsible for ensuring that all of your bluebooks or charts contain your exam number. Do not use your name or any other identifying marks. Number all bluebooks or charts in sequence (e.g., "1 of 4", "2 of 4", etc.), and insert multiple bluebooks or charts within the first bluebook when you are finished.

If you assume any fact "*X*," write "Assuming *X*, ...", and then provide your answer.

You must return this fact pattern along with your bluebooks, in order to receive credit for this examination.

Count the pages of the exam, to make sure that there are three (3) pages after (not including) this cover page.

I wish you the best of luck.

Abel ("**A**") is a college student at State University ("**SU**"). **SU** provides students with access to the school's computer network and free access to the Internet on school-owned computers located in computer rooms around the campus. Students who have their own computers may also access the Internet from their dorm rooms via the school's network. Students access the school system by logging on with a username and password. **SU**'s Terms of Use policy prohibits students from installing software or executing malicious programs on the system.

Late one evening, **A** decides to surf the Internet on a school-owned computer. **A** signs onto America Online's Instant Messenger system (a system that enables users to chat with each other online), and begins instant messaging people online. After several minutes, **A** is messaged by "BeautifulSuzie" ("**B**") whom **A** does not know. The following exchange takes place:

BeautifulSuzie: Hello. What's up?
Abel: Just chatting. Are you really beautiful like your name says?
BeautifulSuzie: Yes.
Abel: How old are you?
BeautifulSuzie: 12. Do you like younger ladies?
Abel: Not really, but we can talk. I go to State University.
BeautifulSuzie: Hey, I live near you. Do you want to get together?
Abel: No. I don't have the time.
BeautifulSuzie: Oh, that's too bad.
Abel: I have to go to sleep. It's very late.
BeautifulSuzie: OK. Would you like a picture of me?
Abel: O.K. My address is Abel@StateUniversity.edu.

B sends an e-mail to "Abel@StateUniversity.edu" to which are attached four digital photographs of a nude girl approximately twelve years of age. In reality, **B** is a lonely 45-year-old single mother. The photos are of **B**'s daughter.

A and **B** communicate several times via e-mail, but **A** has no intention of meeting **B**. However, after much coaxing from **B**, **A** announces that he will meet her by sending an e-mail that says: "O.K., you convinced me to meet you."

Meanwhile, two other **SU** students, Carl ("**C**") and Darryl ("**D**"), who are both computer science majors, plant on several school-owned computers a "Trojan horse," which is a program that secretly records students' user names and passwords when they log onto the system. Twenty students -- include **A** -- log onto the school-owned computers hosting the Trojan horse. The program secretly records the students' user names and passwords. **D** returns later that day and collects the twenty students' logon information.

C also decides to market the Trojan horse program over the Internet. **C** creates a website called "TrojanHorse.com," where he advertises the product. Wishing to expose his software to a wider audience, **C** asks his friend Ezekiel ("**E**"), who owns and operates a website called "Hackers.com," to provide a link to http://www.TrojanHorse.com, which **E** does.

Unknown to **C** and **D**, however, their program contains a serious flaw, which "crashes" those computers onto which the program is loaded. **SU** calls a computer repairman to fix those computers. The repairman fixes the school-owned computers, and charges **SU** $50 per hour for ten hours of work.

C decides to share the student logon information with another **SU** student named Frederica ("**F**"). First, **F** logs onto the **SU** system using **A**'s user name and password. **F** reads **A**'s e-mail. Unknown to **A**, there was another e-mail from **B** to which four more nude photos were attached. **A** had not opened this e-mail, but **F** did.

Second, **F** accesses the account of a student named Greg ("**G**"). **F** finds files in **G**'s account named "**Stolen_Social_Security_Numbers.doc**" and "**Phony_State_Drivers_License_Template.JPG.**" **F** contacts the police and reports both **A** and **G**. Police, interested in initiating an investigation into the matters, tell **F** to "keep up the good work."

Third, **F** accesses the account of Harry ("**H**"), another **SU** student. While looking at **H**'s outgoing e-mail, **F** discovers the following e-mail sent by **H** to Ingrid ("**I**"):

> My Dearest Ingrid:
>
> Nobody cheats me and gets away with it. If I don't get my money, I'm going to kill you and your entire family. I don't care if I have to drive across the country to get you.
>
> Have a nice day,
> Harry

Police investigators are sent to talk to **F**. **F** explains how she accessed the student accounts, and shows them what she had discovered while sifting through the accounts of **A**, **G**, and **H**. While searching the account belonging to **G**, police ask **F** to open another suspicious file entitled "**Fake_ID_Customers.xls**." In that file, **F** and the police find a list of the names of persons to whom **G** had sold false identification. Based on the information provided by **F**, police apply for a warrant to search dorm rooms belonging to **A**, **G**, and **H**, including their personal computers, if any.

While searching **G**'s room, police find a laminating machine, several fake social security cards, and two fake drivers' licenses.

While searching **H**'s computer for evidence of "threatening communications," police discover on **H**'s computer a stolen Jupiter ("**J**") software program that **H** had apparently downloaded from **E**'s "Hackers.com" website.

Assume that all of the parties subsequently learned about the identities and actions of all of the other parties.

QUESTIONS

1. Criminal Offenses
    - 1.1. Who may be charged with criminal offenses by the United States Attorney's Office, and what criminal offenses may each defendant be charged with?
    - 1.2. What maximum prison sentences may be imposed under the relevant statutes? (Note: Disregard the Federal Sentencing Guidelines)
    - 1.3. What are each defendant's substantive defenses?
    - 1.4. What is the government's counterargument to each defense?
    - 1.5. What evidence should arguably be suppressed, and why?

2. Civil Liability
    - 2.1. Who may be civilly liable to whom, and under what theories?
    - 2.2. What are each defendant's defenses?