FINAL EXAMINATION
COMPUTER CRIME
Paul Ohm
December 14, 2009

Instructions:

Please read these instructions carefully before proceeding.

1. The examination consists of seven (7) pages, including the pages containing these instructions. You will find three problems. Please make sure that your copy is complete and that you answer all three problems.

2. This is a take-home examination; you have nine (9) hours to complete the exam. Your answers to the exam must be returned to the Registrar by the time she indicated in the email she used to send this exam. Your answers can be returned electronically via email to cindy.gibbons@colorado.edu or in person. DO **NOT** RETURN YOUR ANSWERS TO PROFESSOR OHM.

3. If you hand in your answers late, I may—at my sole discretion—deduct points or give you a failing grade.

4. If you are typing, you must submit your answers in a computer file with a file format that the Registrar can access on her computer. If the Registrar cannot access your answers, they may not be graded. Recommended file formats are Word 2007 (*.docx); Word 97-2003 (*.doc); Adobe Acrobat (*.pdf); and Rich Text Format (*.rtf).

5. The exam is worth 300 total points. Each problem is worth 100 points, or one-third of the final exam grade.

6. Answers will be graded based on content, clarity of expression, and organization. I suggest that you spend time outlining your response before you start to write. Where information is not provided that would be relevant to the analysis, feel free to explain how different facts would lead to different outcomes.

7. Assume that all cases that were pending when we discussed them in class are still undecided. If any cases have been decided during the course of the semester, you are not responsible for knowing the final rule, result or reasoning, and you will gain nothing by talking about the new decision.

8. You are responsible for the versions of the statutes we studied in this class as they appear in the appendix at the end of the casebook with one exception. For 18 U.S.C. § 1030, you are responsible for the current version, most recently amended in September 2008.

9. In answering these problems, you may consult any written materials you wish. You may also consult electronic materials stored locally on your computer and any materials hosted on our class website, http://paulohm.com/classes/cc09/. You may not use the Internet to discuss the exam or assist you with the exam in any other way.

10. Regardless of when you return the exam, you may not communicate with any other student in our class *for any reason* prior to the time when the exam is due. In addition, you may not communicate with anyone else (e.g. students in other classes, family members, other professors, etc.) about the exam prior to the time when the exam is due.

11. Each problem has a separate word limit, indicated at the beginning of the problem and as follows: Problem One: 1500 words; Problem Two: 1500 words; Problem Three: 750 words. Please put the number of words you write at the end of each answer.

12. If you are handwriting the exam, please write on only one side of each page.

13. Good luck!

Problem One
(100 Points, 1500 Words Maximum)

David has worked for twelve years as a secretary in the marketing department of engineering giant SciTech Industries. Like every employee at SciTech, he has been given access to a computer connected to the company network called the "Unsecured" file server. When David enters his username and password into the login prompt on his office computer every morning, he is automatically given access to his files on the Unsecured server.

When David first started working at SciTech, he signed an employment contract. The contract contained only two sentences about the use of computers and networks in the middle of many pages of other materials: "Please respect the privacy of others on the computer network. Access only the files you are authorized to access." David signed the final page of the contract, beneath the text, "I have read and understand the terms of this employment contract."

SciTech maintains another file server, called the "Restricted" server, intended to be accessed only by those who work in its research and development department. Because the Restricted server houses highly sensitive research materials, SciTech's managers have put in place technical safeguards which limit access only to approved people. They have utilized the most advanced computer access techniques including, among other things, retinal scans and multiple levels of passwords. David has never been given authorization to access the Restricted server.

A few months ago, a SciTech computer support technician accidently misconfigured the Restricted server, creating a link between the Unsecured and Restricted servers. Because of this glitch, any user logged into Unsecured could view some of the files on Restricted. David learns about the glitch from a friend and spends an afternoon taking advantage of it to look through files on Restricted.

David opens dozens of files on Restricted and is horrified to learn about SciTech's covert animal testing research, much of which inflicts what he considers unnecessary pain and death on animal test subjects. He is most shocked to find files containing videos which appear to show mice slowly being crushed to death. Unknown to David, the U.S. Army paid millions of dollars to SciTech to conduct this research, with the goal of developing anti-torture technologies for its captured soldiers.

David shows his direct supervisor one of the videos and voices concerns about the research. The next day, on his way into the building, David is directed to the head of personnel, who tells him that he is being fired for accessing a file server he was not supposed to access, and instructs him to clean out his desk and leave the premises immediately. If David does not leave as quickly as he can, the head of personnel warns, he will be thrown out of the building as a trespasser. David rushes back to his office, boots his computer, enters his username and password, accesses the Restricted files, and copies five of the most graphic mice crush videos to a

portable drive. In a rush to do this, David accidently deletes a folder on the Restricted server. The deleted folder contained critical research results which were not backed up, and as a result of David's actions, researchers have to reproduce months of experiments, at the cost of hundreds of thousands of dollars of researcher time.

David posts the five mouse crush videos to the public video sharing website, YouTube. Thousands of people view the video, and amidst the resulting public outcry, the FBI begins an investigation which leads quickly to David. After the FBI finishes its investigation, the US Attorney obtains an indictment against David charging three criminal counts:

- Count One: Intentionally accessing a computer without authorization or in excess of authorization and thereby obtaining information from a protected computer in violation of 18 U.S.C. § 1030(a)(2)(C). The indictment charges this as a five-year felony under 18 U.S.C. § 1030(c)(2)(B).

- Count Two: Intentionally accessing a protected computer without authorization and as a result recklessly causing damage to a protected computer in violation of 18 U.S.C. § 1030(a)(5)(B) and causing damage and loss in violation of 18 U.S.C. § (a)(5)(C). The indictment charges the (a)(5)(B) charge as a five-year felony under 18 U.S.C. § 1030(c)(4)(A) and the (a)(5)(C) charge as a misdemeanor.

- Count Three: Knowingly possessing a depiction of animal cruelty with the intention of placing it in interstate or foreign commerce in violation of 18 U.S.C. § 48.

18 U.S.C. § 48, which we did not discuss in class, provides in full:

> **§48. Depiction of Animal Cruelty**
>
> (a) Creation, Sale, or Possession.— Whoever knowingly creates, sells, or possesses a depiction of animal cruelty with the intention of placing that depiction in interstate or foreign commerce, shall be fined under this title or imprisoned not more than 5 years, or both.
>
> (b) Exception.— Subsection (a) does not apply to any depiction that has serious religious, political, scientific, educational, journalistic, historical, or artistic value.
>
> (c) Definition.— In this section, the term "depiction of animal cruelty" means any visual or auditory depiction, including any photograph, motion-picture film, video recording, electronic image, or sound recording of conduct in which

a living animal is intentionally maimed, mutilated, tortured, wounded, or killed.

[Note: This is based on an actual statute, but I have simplified and otherwise modified the statute in several ways.]

You are an associate at a criminal defense firm which David has hired to defend him. The partner on the case asks you to write a memo assessing the strength of the government's case against David and the availability and strength of any potential defenses.

Problem Two
(100 Points, 1500 Words Maximum)

Vincent is an FBI agent assigned to a cybercrime squad in New York City. One day, he receives an email from someone calling himself "Ari" who claims that a notorious copyright warez group has been using a password-protected chat room to distribute copies of movies before they are released in theaters. Ari says that the chat room can be found by accessing the hosted-chat.com site on the Internet, entering the chat room called #entourage and using the password "Busey."

From earlier investigations, Vincent knows that the hosted-chat.com site is a free service open to anybody on the Internet which gives users the ability to quickly and easily set up chat rooms to use with friends or strangers. Hosted-chat.com chat rooms can be open to the entire world or password protected. Hosted-chat.com allows so-called "stealth" logins, which permit people to observe conversations invisibly, meaning without having their user name show up in the list of people in the chat room. Vincent logs into the #entourage chatroom in stealth mode. Over the course of an hour, he sees as many as ten people—none calling themselves Ari—chatting about recent movies but not about copying movies. Although hosted-chat.com chat rooms allow users to send and receive files to one another, in the hour he is observing #entourage, Vincent doesn't see anybody transfer any files. He saves a transcript of the entire conversation.

Vincent calls Billy Walsh, the man who administers the hosted-chat.com service, identifies himself to Billy as an FBI agent, and asks about the #entourage chat room. Billy reveals that he had received an email from Ari a month ago similar to the one sent to Vincent, and because he doesn't tolerate criminal behavior on his site, he has been saving transcripts of the #entourage chat room for the entire month. Although Billy does not know the password for the #entourage chat room, he can monitor the conversation in any chat room using his administrator privileges. Billy gives the month's worth of chat transcripts to Vincent. Although the transcripts reveal that users had repeatedly traded files named after recently released movies—QueensBoulevard.divx, Aquaman.divx, Medellin.divx—the transcript does not keep a copy of the files transferred nor record any other details about the transfers.

Vincent asks Billy if users agree to Terms of Service when they join hosted-chat.com, and Billy answers that they do not. Vincent applies for a Pen Register and Trap and Trace Order from a New York federal magistrate judge. He certifies that the surveillance he is requesting is likely to reveal information relevant to an ongoing criminal investigation, and he asks the judge to issue an order allowing Vincent to record the following information for every file transferred in the #entourage chat room for sixty days: (1) user requesting file; (2) user sending file; (3) name of file transferred; and (4) size of file transferred. The judge issues the order, which Vincent serves on Billy and which Billy implements.

At the end of sixty days, the surveillance returns a huge list of files named after recent movies with large file sizes consistent with what one would expect from movie files. Armed with this information, Vincent sends a grand jury subpoena to Billy, asking him for the IP addresses used by two users—named Chase and Drama—who seem to be the heaviest file uploaders. Once again, Billy complies.

The IP address for Chase is owned by MillerGold, a small ISP in California (which is in the Ninth Circuit). Vincent serves a subpoena on MillerGold asking for the name of the user or users associated with the IP address at the time of the incriminating file transfers. MillerGold reveals a user named Eric Murphy. Vincent then obtains a 18 U.S.C. § 2703(d) order from a New York federal magistrate judge ordering MillerGold to produce all basic subscriber information listed in 18 U.S.C. § 2703(c)(2) for Eric Murphy as well as copies of all email messages stored in the MillerGold-hosted email account used by Eric Murphy. MillerGold produces everything requested, including email messages which contain many incriminating statements establishing a massive conspiracy to commit criminal copyright infringement.

The IP address associated with the user named Drama is owned by a Finnish ISP. Vincent calls Agent Lloyd Lee, a Finnish agent based in Helsinki, whom Vincent knows from an earlier case. After describing the investigation, Vincent reads the IP address to Agent Lloyd. One week later, Agent Lloyd sends Vincent not only detailed subscriber information for a Finnish citizen named Turtle Assante but also the contents of Turtle's email account and what appear to be a list of every website visited by Turtle in the past week. All of this evidence implicates Turtle in the conspiracy.

You are the Assistant United States Attorney assigned to Agent Vincent's case. Agent Vincent has asked you to bring an indictment against Eric Murphy and Turtle Assante (whom he hopes to extradite) charging a conspiracy to commit criminal copyright infringement. Write a memo for your bosses assessing whether the investigation violated any statutory privacy laws or the Fourth Amendment. For any potential violations you identify, discuss the remedies available to the defendants.

Problem Three
(100 Points, 750 Words Maximum)

Which federal institution would you prefer to be in charge of setting the rules for **government access to online communications**: Congress or the Judiciary? Support your choice using any type of arguments you see fit, including historical track record; relative inherent institutional strengths and weaknesses; and perceived pro-privacy or pro-law enforcement tendencies. Try to be persuasive. To support your argument, give specific examples from the material we have covered, if helpful.