GEORGETOWN UNIVERSITY LAW CENTER
EXAMINATION IN COMPUTER CRIME
TAKE HOME EXAM

Professor Ohm – Computer Crime

INSTRUCTIONS:

1. This is an OPEN book exam.

2. This six (6) hour exam must be downloaded and submitted using the Online Exam/Paper Management System. This exam will be available beginning Tuesday, April 30, 2013, at 8:30 AM and must be returned by Tuesday, May 14, 2013, at 6:30 PM.

3. There are three problems on the exam. Each question is worth 100 points for a total of 300 points for the entire exam.

4. Each problem has a separate word limit, indicated at the beginning of the problem and as follows: Problem One: 1500 words; Problem Two: 2000 words; Problem Three: 750 words.

5. This exam is final. No clarifications or corrections will be provided. If you believe there is an error, inconsistency, or omission in the exam, please state your assumptions about the issue within your discussion of that issue.

6. You may not identify yourself in any way to the professor as the author of an exam until the grades are published. Therefore, you must remove personal identifying information from your exam document. Failure to remove any personal identifying information is an exam violation which will be referred to the Ethics Counsel. Instructions on how to remove personal identifying information from your take-home exam are available online at http://www.law.georgetown.edu/campus-services/registrar/exams-papers-grades/exams/index.cfm.

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. Once you begin taking this exam, do not talk about the exam, the class, or the subject matter of the class with any other person. After you have submitted your completed exam, do not discuss the exam, the class, or the subject matter of the class with any classmate who has not yet taken the exam.

This exam consists of FOUR (4) pages, including this cover page. Please be sure your exam is complete.

Please be sure that you use your exam number (not your student ID number or social security number).
HONOR STATEMENT

BY SUBMITTING THIS EXAM THROUGH THE ONLINE SYSTEM, I AFFIRM ON MY HONOR THAT I AM AWARE OF THE STUDENT DISCIPLINARY CODE, AND I HAVE NOT WORKED MORE THAN SIX (6) HOURS ON THIS EXAM.

PROBLEM ONE
(100 points; 1500 words)

Perhaps the oddest thing about the situation involving the fired former star employee of Metaverse, Inc., was that nobody at the company had ever seen him in person. They called him Y.T., and they found him five years ago when he answered their online job listing. He’d worked for the company ever since, remotely over the Internet, claiming to be working from home in Russia.

At first, Metaverse hired Y.T. to do relatively unimportant tasks for minimum wage and gave him limited network access to a few files on the company network. But Y.T. proved to be a faithful and talented employee, and over five years, he had earned the trust of Metaverse’s management. In response, the company promoted him many times, giving him more responsibility, better pay, and greater access to sensitive parts of the Metaverse network each time. At the time of the incident, Y.T. was the lead software engineer for the entire company, with full access to almost every single file on the network.

Over those five years, whenever Y.T. received one of his numerous promotions (at least five), human resources would send him a new employment contract, which he always returned signed. Every contract contained a “Confidentiality” clause that provided, in relevant part, “I promise to protect the confidentiality of Metaverse documents, including computer network files. I promise not to disclose any files to anybody unless for Metaverse’s purposes.”

At some point, Y.T. began selling Metaverse files containing important, valuable company information to Metaverse’s competitors. The company suspects Y.T. even sold some files to the Russian government. In media reports, Metaverse’s owner L. Bob Rife has complained, “With his password, Y.T. could get at those files, but he had no business whatsoever within 100 feet of those directories. He knew that, too!”

You are an Assistant United States Attorney in Metaverse’s home district. Metaverse executives have asked you to file a federal indictment charging Y.T. with any crimes he may have committed, in order to facilitate extradition. Write a memo to your boss listing the charges you might bring and assessing the strength of those possible cases, including any arguments you anticipate from defense counsel. Do not discuss any of the following: the extradition process itself, state law crimes, or potential sentences Y.T. might face. Other attorneys in your office are handling these issues.

PROBLEM TWO
(100 points; 2000 words)

You are a federal prosecutor in the district that includes ParkLand, a small national park. One day you are visited by Agent Rana of the U.S. Fish and Wildlife Service field office near ParkLand. He enforces the federal criminal laws prohibiting trafficking in endangered species and is on the trail of someone advertising on the Internet the sale of endangered mountain yellow-legged frogs, which live only in ParkLand.

The case started when Agent Rana received an anonymous tip, a web link to a posting on the popular online service SocialMail. SocialMail bills itself as a hybrid between webmail (web-based email) and social networking services. At its core, SocialMail operates exactly like a webmail service such as Yahoo Mail, Gmail or Hotmail/Outlook. Every user has an “inbox” and can send and receive messages to other users using their email addresses. The difference is that a recipient (and only a recipient) of a
SocialMail message can “socialize” the message by clicking a small “Socialize!” button. This instantly republishes the message onto a completely public part of the SocialMail website, on which the message can be read by anybody, even those who are not logged in to SocialMail. According to its advertising tagline, “It’s like Twitter, but your friends decide what you post!”

By clicking on the link from the tipster, Agent Rana visited a publicly accessible, socialized SocialMail message. It read, in full:

From: RangerD@socialmail.com
To: Paula123@socialmail.com
Subject: endangered tree frog for sale
Date: February 28, 2013 @ 17:35:00 PST

i can sale you a genuine mountain yellow-legged frog for $50. common ingredient for non-traditional medicine. let me know if your interested.

<This message has been SOCIALIZED!>

After reading this message, Agent Rana sent an administrative subpoena to SocialMail’s subpoena compliance office, ordering them to “Produce anything in your records relating to the account RangerD@socialmail.com.” In response, SocialMail produced a copy of the user’s entire private profile, which was blank except for listing a “Name” of “Endangered Frog,” a “Height” of “5 cm,” and a “Weight” of “3 grams.” SocialMail also produced the IP address of the computer that was used initially to create the SocialMail account. Finally, SocialMail produced the entire contents of RangerD’s nearly empty email account, which amounted to a single message in the Sent folder, a copy of the message above. Apparently, no other email messages were stored in the account.

Next, by querying a publicly available, online database, Agent Rana determined that the IP address produced by SocialMail was associated with BigISP. Agent Rana sent another administrative subpoena to BigISP for the user information associated with that IP address at the date and time on the SocialMail message. Much to Agent Rana’s surprise, the IP address was associated with the only ranger station inside ParkLand, the national park.

Agent Rana visited ParkLand’s ranger station and found only one computer, a computer sitting on a desk in the public space, alongside public exhibits with maps and “touch me” wildlife models. Attached to the bottom of the computer’s screen was a small plaque, which read, “For U.S. Park Service Employee Use Only.” Despite the plaque, at the time of Agent Rana’s visit, a non-employee park visitor was at the computer using SocialMail. Hoping for a lucky break, Rana interviewed the visitor, who claimed he had never been to the park before. Rana later verified the visitor’s story.

After asking the visitor to step aside, Agent Rana began using the computer, opening numerous file folders. In one folder called “Human Resources - Confidential,” he found a file called “employee manifest,” and opened it. It listed the names and other employee information for the seven rangers who worked in the station, including one person named “Ranger David Douglas,” who Agent Rana speculates may be RangerD. He also viewed the web browser’s cache files and after some extensive searching found a copy of the SocialMail message that sparked the investigation.

Faced with a seeming dead end, Agent Rana has come to you to help him figure out what he can and should do next, if anything. He would like to set up some monitoring on the network in the ranger station—he’s heard of something called a packet sniffer—to try to catch the culprit in the act of trying to sell endangered animals to other people. He also plans to revisit the ranger station every couple of weeks to check for new information on the computer.

Write a memo to Agent Rana. Assess the investigative steps he has taken so far, highlighting anything he has done that may have violated Constitutional or statutory law. For any potential violations, discuss whether suppression is possible, but do not address other remedies such as discipline or civil liability. Counsel him as to whether he should take any of the investigative steps he proposes. Feel free to offer other avenues for his investigation, if any.
PROBLEM THREE
(100 points; 750 words)

“Guns don’t kill people; people kill people.” So goes the pithy bromide often heard in gun control debates by those opposing new gun laws. In a similar way, in both substantive and procedural computer crime and national security law, we sometimes face hard problems that raise difficult questions about the line between a computer-related tool and the person using the tool. We often ask, how should the law allocate power, culpability, risk, intent, or any other relevant quality between human actors and the hardware and software tools they use? Explain how this “tool versus user” (or alternatively “tool versus toolmaker”) choice should be made in the context of at least one issue or topic we covered this semester.