

Law 8311-001: Computer Crime Seminar

Course Description and Syllabus

Fall 2006

Associate Professor Paul Ohm
University of Colorado Law School

I. Description

This course will explore the legal issues that judges, legislators, prosecutors, and defense attorneys are confronting as they respond to the recent explosion in computer-related crime. In particular, we will consider how crimes in cyberspace will challenge traditional approaches to the investigation, prosecution, and defense of crime that have evolved from our experience with crimes in physical space. Topics will include: the Fourth Amendment in cyberspace, the law of electronic surveillance, computer hacking and other computer crimes, encryption, online economic espionage, cyberterrorism, the First Amendment in cyberspace, federal/state relations in the enforcement of computer crime laws, and civil liberties online. No previous experience is required, although familiarity with the Internet is helpful. Students are required to attend and participate in class sessions, make a class presentation, and write a paper on an approved topic.

II. Course Summary

Overview. This seminar will examine how the criminal justice system responds and should respond to computer-related crime. We will consider three broad questions. First, what conduct should be criminal in cyberspace? Second, what privacy regime should govern law enforcement investigations of computer crime? And third, how should traditional notions of sovereignty that govern the criminal law in the physical world apply in cyberspace?

Timing. The class will meet every Monday in Room 411 from 4:00pm to 5:45pm. Note that we are meeting for five more minutes each week than specified in the course catalog; we are adding time to make up for the Labor Day holiday. I will generally be available for office hours on Monday and Wednesday afternoons from 2:30pm – 3:30pm in Room 433 or at any other time by appointment. I also can be reached via e-mail at paul.ohm@colorado.edu.

Knowledge of Technology. Although no prior level of technical knowledge is necessary, students will be expected to become familiar with Internet technologies and able to discuss the impact of these technologies on the criminal law. Students should ask for clarification anytime an unknown technology is mentioned, and I am happy to schedule formal technology tutorial sessions if needed.

Paper. Students are required to write a twenty-five to thirty page paper (reasonable font and margins; double-spaced). The paper should represent an original work of scholarship that analyzes in an original and creative way one or more of the issues that we discuss in class. Each class

addresses a topic that provides a potential starting point for papers. Although I will permit students to choose a paper topic outside of the issues covered in class (upon approval and only within reason), most of students should choose a topic covered in class as a point of departure for the paper.

Topics must be selected and submitted to me for approval by the start of class, Monday, September 25, 2006. Outlines and rough drafts may be submitted to me for review at any time prior to one week before the final due date. This is strongly encouraged; in my experience, close consultation with a supervising professor is the best way for a student to improve a paper (and a paper's grade.) Papers are due by the start of the last class, Monday, December 4, 2006. To recap, the key deadlines for the paper are:

Monday, September 25, 2006	Paper Topics Due by Start of Fourth Class
Monday, November 27, 2006	Last Day to Submit Outlines or Rough Drafts for Review
Monday, December 4, 2006	Papers Due by Start of Class

Participation. Students are required to take an active role in classroom discussions. As in any seminar, very little material will be presented through lecture, and every student must contribute to a lively conversation. Classroom participation may account for as many as three points—plus or minus—in the final grade.

In addition to taking an active role in weekly in-class discussions, students must fulfill a second participation requirement in one of two ways: First, students can opt to present their final paper to the class during the last two classes of the semester. These presentations will run from ten to fifteen minutes, including time for questions.

Alternatively, students can choose to publish responses to two weeks' worth of reading. A response can take one of two forms: (1) a response memo, approximately two pages, double-spaced; or (2) a "podcast"—glorified techspeak for a digital recording of your voice—approximately five minutes long. In either format, a student response should provide commentary about some of the reading for the upcoming week. Responses should be posted to the class website no later than Noon, the day before class. In addition, all students are expected to have read or listened to each week's student responses before coming to class.

At the second class, on Monday, September 11, 2006, students will be asked to commit to either present their papers or respond to the reading. For those students choosing the response option, sign-up sheets will be completed that day to ensure that student responses are spread throughout the semester. Students choosing the response option need not decide whether to write a memo or record a podcast in advance.

So long as paper presentations and responses reflect conscientious and thoughtful efforts to complete the assignments, they will not be graded for their relative merit. Conversely, students who fail to present their paper or submit their responses or who complete these tasks with evidently little

thought or preparation will lose up to two points from their final grade. This is in addition to the possible three point bonus or penalty for general class participation.

The class response blog is online at computer_crime.classcaster.org. Directions for posting response memos and response podcasts are available at the class website: paulohm.com/classes/cc06.

Reading. The required books for the class are the pre-publication draft of *Computer Crime Law*, a forthcoming casebook edited by Professor Orin Kerr of the George Washington Law School, and *Who Controls the Internet?* by Jack Goldsmith and Timothy Wu.

Professor Kerr's casebook is due to be released sometime this fall. For the time being, photocopies of the chapters of the book will be provided on a week-by-week basis through the Faculty Assistants. Once the book has been published, these copies will no longer be available.

Because this area of the law is always evolving, I expect to supplement the materials identified above as new cases, articles and other reading materials are published. I also may invite guest speakers for certain topics.

Other Resources. Two somewhat dated but still useful general background texts written by technologists are:

Bruce Schneier, Secrets and Lies: Digital Security in a Networked World ("Schneier") (2000).

Dorothy E. Denning, Information Warfare and Security ("Denning")(1999).

At several points in the syllabus below, I have assigned as optional reading pages from these books for students interested in further background reading.

If you want to be diverted for a long afternoon, a good "true crime" story about an early computer crime is:

Clifford Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (1989).

Several bloggers post frequently about information privacy or computer crime:

Orin Kerr (GW Law Professor): www.orinkerr.com and www.volokh.com

Dan Solove(GW Law Professor): www.concurringopinions.com

Ed Felten (Princeton Computer Science Professor): freedomtotinker.com

Bruce Schneier (Computer Security Expert): schneier.com/blog

Declan McCullagh (Journalist): <http://www.politechbot.com/>

In print, the New York Times quite often runs stories about computer crime. In addition, at news.com, C|Net runs many computer crime-related stories. Pay attention to articles authored by

Declan McCullagh.

The Yin and Yang for press releases and analysis related to recent computer crimes are:

U.S. Department of Justice's Computer Crime and Intellectual Property Section (CCIPS):
www.cybercrime.gov.

The Electronic Frontier Foundation: www.eff.org.

"The Source" for (one side's view of) the law of search and surveillance online is a CCIPS publication entitled, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" available online at <http://www.cybercrime.gov/s&smanual2002.htm>.

Grading. The grade that each student receives for his or her paper will provide the primary basis for his or her grade in the seminar. However, as detailed above, classroom participation and the mandatory presentation or responses will also play a role. Strong participation will increase a final grade by up to three points. (e.g. from 88 to 91). Poor participation will decrease a grade by up to three points. Insufficient responses or poor presentations will decrease a grade by up to another two additional points.

Course Updates. Course updates will be available on our course TWEN site and also at <http://paulohm.com/classes/cc06/>.

III. Week-by-week Syllabus

For each week listed below you will find a list of questions to introduce the week's themes and to help motivate paper topic ideas; the required reading for the week; a list of "technology topics" that will be discussed in class; and a list of other related reading. If you are unfamiliar with any of the technology topics listed below, try at least to find a definition of the unknown term before coming to class. Wikipedia (en.wikipedia.org) is an unexpectedly good resource for gentle introductions to technical topics.

Monday, August 28, 2006

Week 1: Introduction to Computer Crime

In the first week, you will be introduced to the nature and scope of the computer crime problem. Just what do we mean by "computer crime"? How is computer crime different from traditional crime? How should we draw analogies between physical space and the Internet? Should federal and state criminal law extend to the bits and bytes of the Internet, or should the Internet be governed by its own rules? Are computer crimes inherently less objectionable than their equivalents in physical space? Is the Internet inherently less conducive to a regime of civil liberties against law enforcement monitoring versus physical space, or more?

Readings:

Kerr, Computer Crime Law, Chapter 1, 1-6.

First supplemental reading (available at <http://paulohm.com/classes/cc06/>).

Technology Topics:

IP Addresses; Domain Name System; the Internet; the World Wide Web.

Other Suggested Sources:

Bruce Schneier, Secrets and Lies: Digital Security in a Networked World ("Schneier") (2000), pages 1-58, 176-187, 202-211

Dorothy E. Denning, Information Warfare and Security ("Denning") (1999), Pages 203-258, 269-281.

Monday, September 4, 2006

No Class: Labor Day

Monday, September 11, 2006

Week 2: Computer Misuse

Week 2 begins a two-week discussion concerning what kinds of conduct online should be made and are criminal. This week addresses computer misuse such as computer hacking and the dissemination of computer viruses. Has the hacker community that seeks to legitimize non-malicious hacking discovered truths about the nature of cyberspace, or are they endorsing electronic vandalism? Should it be legal for a victim to “hack back” and disable a computer that has launched an attack against it (a sort of cyber-self-defense)? Similarly, how should the legal system treat the intentional spread of computer viruses? Do traditional assault and battery principles suffice, or are virus crimes impossible to analogize to traditional crimes from physical space? What is the current statutory framework for evaluating illegal activity online? Should Congress pass separate computer crime statutes, or simply amend present statutes to include crimes committed over the Internet?

Readings:

Kerr, Computer Crime Law, Chapter 2, 7-42; 81-104.

Goldsmith and Wu, Who Controls the Internet? Chapter xx, pages xx

Technology Topics:

Network Security; Viruses, Worms, Trojan Horses; Denial of Service.

Other Suggested Sources:

Denning, 43-76

Schneier, pages 151-175

Monday, September 18, 2006

Week 3: Computer Misuse: Unauthorized Access

In Week 3, we will continue the discussion of computer misuse from Week 2, focusing on the concept of “unauthorized access” to a computer, which has found a way into many statutes around the country. Should contract or user policy play a role in whether access is unauthorized and thus potentially a criminal act? Do some statutes over-criminalize conduct online? If so, how should they be amended?

Readings:

Kerr, Computer Crime Law, Chapter 2, 42-71.

Handout on Harvard Business School “Hack” (available on website).

Handout on Wireless Access Point Theft Indictments (available on website).

Technology Topics:

Administrator/root Access; Website security (passwords, unlinked URLs).

Monday, September 25, 2006

Week 4: Traditional Crimes on Computer Networks and the First Amendment

In Week 4, we will begin to look at the use of computer to commit more traditional crimes with an emphasis on the First Amendment. The class will consider the normative criminality of online threats, cyberstalking, electronic monitoring, child pornography, obscenity, and other acts. After considering each case, we will look for broader principles: Could the overcriminalization of conduct on the Internet threaten the freedom and free expression of Internet users? Would undercriminalization lead to anarchy? Can we articulate general principles for how to apply traditional crimes on the Internet, or is each case unique? Should intangible acts be criminalized if no tangible harm results? If so, what should such a law look like?

Reminder: Paper Topics Due by Start of Class

Readings:

Kerr, Computer Crime Law, Chapter 3, Economic Crimes (105-126); Crimes Against Persons (143-158); Child Pornography (181-219). [Note: The length of the assignment will most likely be reduced.]

Technology Topics

Inter-Relay Chat (IRC).

Other Suggested Sources:

Denning, pages 90-100.

Monday, October 2, 2006

Week 5: Punishment

In Week 5, we will consider what kind of sanctions the legal system should impose for committing computer crimes. For example, how should juvenile hackers be punished, if at all? How should the legal system punish invasions of privacy? Is it cruel or counterproductive for the legal system to impose prison sentences for computer hacking? Alternatively, is it institutionally racist to impose light penalties on computer hackers (who are almost exclusively white) when the same legal system imposes draconian mandatory prison sentences on crack cocaine dealers (who are mostly nonwhite)? Should convicted felons be prohibited from using a computer during the period of supervised release? We will examine these texts and discuss whether the current distinctions make sense as matter of policy and politics.

Readings:

Kerr, Computer Crime Law, Chapter 4: 220-250.

Monday, October 9, 2006

Week 6: Hands-On Technology Lab

In Week 6, we will move for one class to a computer lab across campus operated by the Interdisciplinary Telecommunications Program for a hands-on tutorial about the computer crime techniques and programs you are studying. In particular, in preparation for the second phase of the class, we will practice using technologies that mask and reveal private information online such as encryption, packet sniffers, TOR (The Onion Router), password crackers, and steganography.

Readings:

Handout.

Monday, October 16, 2006

Week 7: The Fourth Amendment and Stand-Alone Computer Devices

Week 7 begins the second phase of the seminar, devoted to civil liberties online and the privacy regime that should govern law enforcement investigations in cyberspace.

In week 7 we will study the Fourth Amendment as it applies under current law to cases involving stand-alone computers (as opposed to the Internet). We look at what constitutes a search and seizure, when is a warrant required before government can look through files stored on a computer, and what exceptions apply to the warrant requirement.

Readings:

Kerr, Computer Crime Law, Chapter 5, 251-290; 297-332.

Technology Topics:

Computer Storage; Basic Computer Forensics Principles.

Monday, October 23, 2006

Week 8: The Fourth Amendment and the Internet

In week 8, after reviewing how the courts have applied the Katz "reasonable expectation of privacy" test and the exceptions to the warrant requirement in computer cases, we will focus on three largely unresolved issues that form the core of Fourth Amendment doctrine in cases involving the Internet. We look to the development of the law of privacy from the early days of the

telephone network to the rapid expansion of the Internet.

Readings:

Kerr, Computer Crime Law, Chapter 5, pages 332-379.

Technology Topics:

E-mail; FTP; Internet Routing.

Monday, October 30, 2006

Week 9: Internet Surveillance and ECPA, Part I: Realtime Surveillance--Title III and the Pen Register/Trap and Trace Act.

Week 9 of the course examines the legal regime governing electronic surveillance on the Internet, and in particular 15 U.S.C. 2510-22, also known as "Title III." Title III places a blanket ban on eavesdropping (subject to certain narrow exceptions) both in real space and the Internet. The discussion focuses first on understanding how Title III works in cases involving the Internet. For example, is "Carnivore" consistent with Title III? Does Title III give computer hackers a right to be free from monitoring of their trespasses into victim computer networks? Does it matter whether the monitoring is conducted by the system administrator of the victimized network to protect the network, versus by law enforcement in an effort to bring criminal charges against the hacker? Do warning banners that pop up as users log on to government networks create implied consent to monitoring, eliminating Title III rights? Does a user who sees the banner but does not read it also consent to monitoring? What about a hacker that breaks into the network through a back door and never sees the banner: has he also consented to monitoring?

The second half of the class will consider whether Title III, written in the 1960s to protect private telephone conversations in the wake of Berger, makes any sense when applied to monitoring life on the Internet. On one hand, we cherish our privacy on the Internet just as much as in our telephone conversations, so it seems logical to use the same legal framework to protect privacy rights in both contexts. On the other hand, the Internet permits a far broader range of activity than mere communication, and it may not work to offer a blanket privacy protection over all Internet communications as we have for all phone conversations. Should we scrap Title III and devise an entirely new regime to govern electronic surveillance in cyberspace? If so, what should it look like?

Readings:

Kerr, Computer Crime Law, Chapter 6, 380-428.

Goldsmith and Wu, Who Controls the Internet?, Chapter 4. [Background]

Technology Topics:

Packet sniffers; packet headers.

Monday, November 6, 2006

Week 10: Internet Surveillance and ECPA, Part II: Stored Communications Act.

The stored communications portion of the Electronic Communications Privacy Act (18 U.S.C. 2701-11) was enacted by Congress in 1986 to fill in the gaps created by the uncertain application of the Fourth Amendment in cyberspace. In Week 10, we will study the statute and consider how successfully it achieves its goal of creating parity between privacy rights in the physical world and in cyberspace. The first half of the class will be purely descriptive: how does the Electronic Communications Privacy Act (ECPA) work? For example, how can the FBI obtain account records from Internet service providers? When can the FBI obtain a suspect's e-mail? When can an Internet service provider disclose a customer's e-mail or account information to the government?

In the second half of the class, we will consider how well ECPA achieves its goals. For example, does ECPA protect Internet privacy rights sufficiently? Is the distinction between “remote computing service” and “electronic communication service” that pervades ECPA a viable one? Can a statutory framework designed in 1985 match the Internet technology of 2000, or is ECPA hopelessly outdated? If the latter, how should ECPA be amended to reflect technological change and current conceptions of Internet privacy? How does our experience with ECPA shed light on whether the Fourth Amendment or a statutory regime can best protect privacy on the Internet?

Readings:

Kerr, Computer Crime Law, Chapter 6, pages 428-456.

Technology Topics:

Logfiles; Webmail (Yahoo!, Gmail, Hotmail) versus Desktop e-mail; Search engines.

Monday, November 13, 2006

Week 11: National Security, FISA, and the NSA Wiretapping Program.

In Week 11, we will examine the government’s use of network surveillance and monitoring to protect national security against threats from other nation-states and terrorist organizations. Although much of this type of monitoring involves possible criminal activity, often the goal is to detect and disrupt the threat rather than to collect evidence for a criminal trial. What is the structure of the Foreign Intelligence Surveillance Act (FISA) and how does it differ from the ECPA? Is the FISA Court a rubber-stamp on executive authority? Does the NSA Wiretapping Program, revealed in late 2005, violate statutory law or the Constitution?

Readings:

Kerr, Computer Crime Law, Chapter 8, pages 544-575.

Handouts on NSA Wiretapping Program.

Monday, November 27, 2006

Week 12: Jurisdiction.

In Week 12, we examine the inherently cross-border nature of computer crime. A computer criminal can sit in California, route his communications through servers in Virginia and Washington State, to attack a victim in Colorado. Who is empowered to investigate and prosecute these crimes? Are the police constrained by search and seizure laws from reaching across state lines for evidence? Should state law enforcement agencies defer in cases such as these to Federal investigators? All of these problems are magnified when crimes cross International boundaries. Are some International crimes inherently unregulable? What are the effects of international treaties that seek to harmonize computer crime law?

Readings:

Kerr, Computer Crime Law, Chapter 7, pages 457-76; 496-521.

Goldsmith and Wu, Who Controls the Internet?, Chapters 5 and 10.

Technology Topics:

Encryption; Steganography.

Monday, December 4, 2006

Week 13: Sum-up and Class Presentations