Computer Crime Law Syllabus

Law 278.78
Fall 2013
Mondays and Wednesdays 11:20-12:35
3 Credits
Boalt Hall Room 12
Course Control Number: 49679

Chris Jay Hoofnagle
344 Boalt North Addition
Berkeley, CA 94720
510-643-0213
choofnagle@law.berkeley.edu

Course Description

"Computer crime" has been with us since the 1960s, but our society's dependence upon, and the evolution of, networked communications has changed computer crime dramatically in recent decades. With the aid of a computer, individuals now can levy sophisticated attacks at a scale typically available to organized crime rings or governments. As a result, all 50 states and the federal government have enacted laws prohibiting unauthorized use of computers, and in recent years, governments have tried to harmonize these laws internationally.

Computers can be the means, target of, or the source of information about a crime, and increasingly, those interested in all aspects of criminal law must have some working knowledge of computer crime to effectively investigate, prosecute, and defend cases. This course will explore the policy and law of computer crime and consider how "cybercrimes" are different from and similar to transgressive behavior in physical space. Topics will include the Fourth Amendment, forensics, electronic surveillance, cyberbullying, identity theft, computer hacking and cracking, espionage, cyberterrorism, privacy, the era of “forced disclosure,” and the challenge of cross-jurisdiction enforcement.

Texts

Required for the Course

Thomas K. Clancy, Cyber Crime and Digital Evidence: Materials and Cases, First Edition 2011, LexisNexis, ISBN: 9781422494080

Please note: there is a heavily-discounted loose-leaf version of the textbook with the same contents and pagination. ISBN: 9781422495995

Optional for the Course

Joseph Menn, Fatal System Error (PublicAffairs) ISBN: 9781586487485

Kevin Poulsen, Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground (Crown) ISBN: 9780307588685

All other optional readings are on bSpace

You might find these resources helpful:

- Cybercrime Review—the best blog on computer crime: http://www.cybercrimereview.com/
- National Institute for Justice, Investigations Involving the Internet and Computer Networks (2007)
- Twitter: follow @thehackernews, @th3j35t3r
- Jeff Fischbach's Hazdat: http://hazdat.com/
- Susan Brenner's Cyb3rcrime: http://cyb3rcrim3.blogspot.com/
- Robert Cannon's Cybertelecom: http://www.cybertelecom.org/
- CCIPS, Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations: http://www.cybercrime.gov/ssmanual/index.html
- CCIPS, Prosecuting Computer Crimes: http://www.cybercrime.gov/ccmanual/index.html

Grades

Your grade will be determined based upon the final exam (80%) and classroom discussion, which consists of day-to-day discussion and a 20-minute presentation on a topic related to computer crime (20%).

The final exam will be a take-home, open-book exercise. Once you start this exam, you must complete it within 8 hours. This work must be your own. You should not discuss or work with anyone else during the exam administration period. Unless you are 100% certain that there is a serious error on the exam, you should assume that ambiguities and strange facts are part of the challenge, and you should work through it on your own. If you email me with an exam question, I will post it and a response to the class list.

Developing oral advocacy skills is a very important element in legal education, however, many students have few opportunities to engage in public speaking. Your classroom presentation will give you an opportunity to give a 20 minute summation of an issue in computer crime law. Some topics are more technically focused than others, but remember that as an attorney, one of your main functions is to educate others—opposing counsel, judges, and juries—about your client's situation, and that this education will often focus upon the particularities or customs of your client. Pretend that the class is a jury or a judge, and you are tasked with explaining this topic with credibility and fairness.

Please choose from this list and reserve the topic with Chris, or suggest your own topic.

- Workplace monitoring (extent of and types employed)
- Encryption
- Types of search protocols
- Compelling passwords
- Security breach notification
- IP Addresses, subscriber info, URLs, Web Addresses
- Border searches
- Child pornography: distribution
- Child pornography: possession and viewing

- Child pornography: proving image is a real child
- Social networking sites and child predators
- Online methods to commit copyright violations
- Spyware
- Phishing
- Spam
- Identity crimes
- Cyberbullying
- Threats
- Cyberstalking
- Defamation
- Sentencing enhancements
- Sentencing and child pornography
- Sentencing and banning internet use
- The conficker worm
- Stuxnet and flame
- The NSA's Terrorist Surveillance Program, PRISM, and related programs

Because of the size of this class, participation is very important. Please read for each class and be prepared to discuss the material.

Attendance

Since you are an adult, you can choose to attend or not. However, being absent cannot be good for the 20% of your grade that depends upon in-class discussion.

Office Hours

I will set office hours soon. I am happy to meet with you any day of the week. Just email me. My office is 344 Boalt North Addition.

Events

Berkeley is a center for the study of computers and privacy law. You might be interested in optional events during the semester, the most salient of which are included in the class schedule below. The TRUST Seminar meets on Thursdays at 1 on North Campus. Many of these seminars are relevant to this class, and there's free lunch:

http://www.truststc.org/seminar.htm

Schedule of Classes

Date	Class	Assignments (all non-textbook readings are on bSpace)
1: W 8/21	Introduction: the problem of computer crime	Textbook: 1-5 On bSpace: -Jason Franklin et al., *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*, 2007. -Ross Anderson, *Why Information Security is Hard–An Economic Perspective*. -Caroline Eisenmann, *When Hackers Turn to Blackmail*, HBR Case Study, October 2009
2: M 8/26	Digital Evidence	Textbook: 7-20 On bSpace: -Richard Clayton's *Anonymity and traceability in cyberspace*, PDF pages 1-19
3: W 8/28	The Fourth Amendment "Inside the Box"	Textbook: 21-35 Optional: The 21st Century Genesis of the Bad Leaver
M 9/2	Labor Day No Class	
4: W 9/4	The Fourth Amendment: Private Searches	35-47 Optional: Defending Privacy at the U.S. Border: A Guide for Travelers Carrying Digital Devices

5: M 9/9	The Nature of Digital Searches	49-89
6: W 9/11	Warrants for Digital Evidence	109-127 Optional: Security Minded Drive Encryption
7: M 9/16	Search Execution Issues	89-108, 129-134
W 9/18	Class Cancelled: Chris at ALI	
8: M 9/23	Consent Searches and Passwords	141-165
9: W 9/25	Wireless Phone Searches	167-187 Optional: Warrant to Unlock Google Phone
10: M 9/30	Seizures of Digital Evidence	189-211 -Jones decision on bSpace Optional: Discussion of Gorshkov case in Kingpin

11: W 10/2	Computer Networks and other “outside the box” issues	225-256 Optional: Facebook search warrant; Yahoo compliance guide; Sprint compliance guide; NIJ Internet investigations
Makeup F 10/4	Major internet security events: the conficker worm, stuxnet and flame, the NSA TSP/PRISM	Mark Bowden, The Enemy Within, The Atlantic, June 2010 Michael Joseph Gross, A Declaration of Cyber-War, Vanity Fair, April 2011 James Risen and Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, The New York Times, Dec. 16, 2005. Optional: NSA and Crypto AG
12: M 10/7	Statutory Protections: Pen Register / Trap and Trace Statute / The Wiretap Act	257-268 Optional: Twitter 2709 Order
W 10/9	Class cancelled—Chris at NSF—TRUST	
13: M 10/14	Statutory Protections: The Stored Communications Act	269-305
14: W 10/16	Obscenity and Child Pornography: speech issues	307-336; 340-347 Optional: Emily Bażelon, The Price of a Stolen Childhood,

		New York Times Mag., Jan. 2013
15: M 10/21	Child Pornography	347-376 Optional: Child Molester Behavioral Analysis
16: W 10/23	Child Pornography: search and seizure; sexting	377-409 Optional: The ‘Butner Study’ Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders

17: M 10/28	Exploitation of children via the internet	411-437 Optional: Rachel Aviv, The Science of Sex Abuse, The New Yorker, Jan 14, 2013
18: W 10/30	Using property crimes to address computer misuse	439-452
Makeup F 11/1	State Actors and Computer Crime: Computer Espionage	The Mandiant Report Dave Shackleford, Why Your Organiation Needs a Travel Security Program and How to Build One
19: M 11/4	Computer Fraud and Abuse Act	453-486 Optional: CRS CFAA Overview
20: W 11/6	CFAA continued	486-509 Optional: Lori Drew Indictment
M 11/11	Veterans Day No Class	
21: W 11/13	Intellectual property crimes	511-546 Optional: Does Cybercrime Really Cost 1 Trillion?
22: M 11/18	Malware and Spam	547-570 Optional: Meet The Hackers Who Sell Spies The Tools To Crack Your PC, The Cybercrime Black Market; The Business of Rogueware

23: W 11/20	Identity crimes and threats	570-596 Optional: Selection from "We Are Anonymous" Optional: Jason Andress, Doxing and Anti-Doxing, Information Reconnaissance for the Stalker and the Stalked
24: M 11/25	Cyberstalking and defamation	596-621 Optional: Danielle Citron, Law's Expressive Value in Combating Cyber Gender Harassment
TBD	Review Session	
Th 12/5	Final Exams Available	
F 12/13	Final Exams Due	