

Cyber Crime Course
Course Description and Syllabus
University of Oregon School of Law
Spring Semester 2008
Adjunct Professor Sean B. Hoar
sean.hoar@usdoj.gov
541-465-6792 (voice)
541-465-6917 (fax)

I. Course Description

This two-credit course will explore the legal issues affected by on-line crime. The course is taught from the perspective of a practicing attorney who deals with these issues on a daily basis. The course will examine the evolution of criminal law relative to the development of new technology. In doing so, it will examine four primary areas: (1) technology relevant to on-line crime; (2) conduct criminalized in cyberspace, (3) privacy laws governing law enforcement investigations in cyberspace, and (3) the implications of cyber crime upon traditional notions of sovereignty. Topics will include: the evolution of cyber crime; forensic analysis of digital evidence; on-line investigative techniques; the Fourth Amendment in cyberspace; the law of electronic surveillance; federal statutes proscribing on-line crime; and on-line crime trends, including identity theft, Internet fraud, and new technologies affecting on-line crime.

Given the rapid changes in technology, and the corresponding changes in the means by which on-line crime is committed, investigated, and prosecuted, the course will regularly include discussions of current events. There are no prerequisites, and there will be a final examination. In an attempt to reduce the stress surrounding the final examination, however, 40% of the grade will be determined by in-class participation prior to the final examination. Of this 40%, 10% will be determined by class attendance and weekly participation. The remaining 30% will be determined by the preparation and delivery of a small group class presentation on one of ten topics, as further explained during the first class session.

II. Course Summary

Of the thirteen sessions which comprise this course, the first three will discuss Internet and computer technology relevant to cyber crime. The next five classes will examine conduct criminalized in cyberspace. The next four classes will examine the privacy laws governing law enforcement investigations in cyberspace. The final class will examine the implications of cyber crime upon traditional notions of sovereignty. The required reading in this course will be from relevant case law and law review articles contained in this syllabus and available on-line.

III. Week-by-week Syllabus

A. **Week 1 (January 8th): Introduction to “Cyber crime”**

The first week will serve as an overview for the course and provide an introduction to the nature and scope of computer crime. The class will include a presentation about “the dark side of the Internet - untamed frontiers (bots, spam, hijacked addresses, unauthorized access to and disclosure of personally identifiable information, compromised systems and other nightmares . . .).” The class will also involve an explanation of team presentations on topics from week 4 through week 13 of the course.

Readings:

Sean B. Hoar, *Trends in Cybercrime: The Dark Side of the Internet*, ABA Criminal Justice Magazine, Fall 2005; Vol. 20, No. 3.

Jason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage, *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*, Computer and Communications Security, October 29 - November 2, 2007.

B. **Week 2 (January 15th): Computer forensics and on-line investigative tools – tracing and recovering electronic evidence**

This class will include a presentation on computer technology as it pertains to the creation of digital evidence and the importance of computer forensic examinations.

Readings:

Paul H. Luehr, *Real Evidence, Virtual Crime: The Role of Computer Forensic Experts*, ABA Criminal Justice Magazine, Fall 2005; Vol. 20, No. 3.

C. **Week 3 (January 22nd)Unauthorized access to computers – a demonstration of how computer system intrusions occur, and what can be done to prevent and detect them**

This class will include further discussion about the importance of computer forensic examination, and where digital evidence may be found.

D. **Week 4 (January 29th): The criminalization of unauthorized access to computers – a discussion of the applicable federal statutes.**

This class will include a presentation about the federal statutes proscribing and punishing conduct involving computer intrusions, and relevant case law.

Readings:

Federal statute: 18 U.S.C. §§1030 (computer fraud) and 1037 (CAN-SPAM Act);
United States v. Morris, 928 F.2d 504 (2nd Cir.), cert. denied, 502 U.S. 817, 112 S.Ct. 72

(1991);
United States v. Sablan, 92 F.3d 865 (9th Cir. 1996);
International Airports Centers, L.L.C., v. Citrin, 2006 U.S. App. LEXIS 5772 (7th Cir.,
March 8, 2006);
United States Sentencing Guidelines § 2B1.1.

E. Week 5 (February 5th): The criminalization of on-line identity theft – a discussion of the applicable federal statutes – and what preventive measures can be taken.

This class will include a presentation about the federal statutes proscribing and punishing conduct involving identity theft, and relevant case law.

Readings:

Federal statutes: 18 U.S.C. §§ 1028(a)(7) (identity theft) & 18 U.S.C. 1028A (aggravated identity theft);
United States v. Williams, 355 F.3d 893 (6th Cir. 2003);
United States v Melendrez, 389 F.3d 829 (9th Cir. 2004);
United States v. Sash, 396 F.3d 515 (2^d Cir. 2005);
Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 Or L. Rev. 1423 (2001);
United States Sentencing Guidelines § 2B1.1.

F. Week 6 (February 12th): The criminalization of Internet fraud/access device fraud/threatening communications/interstate stalking – a discussion of the applicable federal statutes.

This class will include a presentation about the federal statutes proscribing and punishing conduct involving Internet fraud/access device fraud/ threatening communications/interstate stalking, and relevant case law.

Readings:

Federal statutes: 18 U.S.C. §§ 875 (interstate extortion/threatening communications), 1343 (wire fraud), & 2261A (interstate stalking);
United States v. Kammersell, 196 F.3d 1137 (10th Cir. 1999);
United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997);
United States v. Bowker, 372 F.3d 365 (6th Cir. 2004);
United States Sentencing Guidelines §§ 2A6.1, 2A6.2, & 2B1.1.

G. Week 7 (February 19th): The criminalization of copyright infringement/economic espionage/trade secret theft – a discussion of the applicable federal statutes.

This class will include a presentation about the federal statutes proscribing and punishing conduct involving copyright infringement/economic espionage/trade secret theft, and relevant case law.

Readings:

Federal statutes: 18 U.S.C. § 2319 (copyright infringement) & 17 U.S.C. § 506 (copyright infringement); 18 U.S.C. §§ 1831 (economic espionage) & 1832 (trade secret theft);

United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994);

A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001);

MGM Studios Inc. v. Grokster, Ltd., 125 S. Ct. 2764 (2005);

Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 Wash. U.L.Q. 835 (1999);

United States Sentencing Guidelines §§ 2B1.1 and 2B5.3.

H. Week 8 (February 26th): The criminalization of child exploitation and child pornography – a discussion of the applicable federal statutes.

This class will include a presentation about the federal statutes proscribing and punishing conduct involving child exploitation and child pornography, and relevant case law.

Readings:

Federal statutes: 18 U.S.C. §§ 2252 & 2252A (child pornography); 18 U.S.C. § 2422(b) (using the Internet to entice sexual activity); 18 U.S.C. § 2423(b) (traveling in interstate commerce with the intent to engage in criminal sexual activity);

Ashcroft v. Free Speech Coalition, 535 U.S. 234, 122 S.Ct. 1389 (2002);

United States v. Adams, 343 F.3d 1024 (9th Cir. 2003);

United States v. McCoy, 323 F.3d 1114 (9th Cir. 2003);

United States v. Gourde, — F.3d —, 2006 Westlaw 574302 (9th Cir. March 9, 2006);

United States Sentencing Guidelines §§ 2G1.3 & 2G2.2.

I. Week 9 (March 4th): Electronic evidence and the Constitution – a discussion of how the Fourth Amendment applies to on-line conduct.

This class will include a presentation about the Fourth Amendment to the United States Constitution and its application to on-line conduct.

Readings:

Rule 41 of the Federal Rules of Criminal Procedure and Mobile tracking device statute:
18 U.S.C. § 3117;

Olmstead v. United States, 277 U.S. 438, 48 S.Ct. 564 (1928);

Berger v. New York, 388 U.S. 41, 87 S.Ct. 1873 (1967);

Katz v. United States, 389 U.S. 347, 88 S.Ct. 507 (1967);
Kyllo v. United States, 533 U.S. 27, 1215 S.Ct. 2038 (2001);

J. Week 10 (March 11th): Intercepting communications – a discussion of how Title III of the Omnibus Crime Control and Safe Streets Act of 1968 applies to on-line conduct.

This class will include a presentation about the federal wiretap statute and its application to on-line conduct.

Readings:

Selected federal statutes pertaining to wiretapping: 18 U.S.C. §§ 2510-22;
Selected federal statutes pertaining to pen registers and trap and trace devices: 18 U.S.C. §§ 3121-27;
United States v. Seidnitz, 589 F.2d 152 (4th Cir. 1978);
Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577 (1979);
United States v. Smith, 155 F.3d 1051 (9th Cir. 1998);
Fraser v. Nationwide, 135 F.Supp.2d 623 (E.D. Penn. 2001);
Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002);
United States v. Councilman, 418 F.3d 67 (1st Cir. 2005);

K. Week 11 (March 18th): Electronic Communications Privacy Act – a discussion of how electronic records can be obtained by the government.

This class will include a presentation about the Electronic Communications Privacy Act and its application to on-line conduct.

Readings:

Selected federal statutes pertaining to stored communications (the Electronic Communications Privacy Act): 18 U.S.C. §§ 2701-11;
United States v. Reyes, 922 F.Supp. 818 (S.D. NY 1996);
Bohach v. Reno, 932 F. Supp.1232 (D. Nev. 1996);
McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998);
Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994);
United States v. Kennedy, 81 F.Supp.2d 1103 (D. Kansas 2000);
Quon v. Arch Wireless Operating Co., Inc., 309 F.Supp.2d 1204 (C.D. Cal. 2004);

March 24th through 28th is Spring Break so there will be no class.

L. Week 12 (April 1st): The USA PATRIOT Act – a discussion of recent legislation, including the USA PATRIOT Act, and how it applies to electronic evidence.

This class will include a presentation about the USA PATRIOT Act and its application to on-line conduct.

Readings:

Selected federal statutes pertaining to the USA PATRIOT Act;
In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002);

- M. Week 13 (April 11th): Sovereignty in cyber space – a discussion of how international, federal, and state relations are impacted by cybercrime; review for final exam.**

This class will include a presentation about how the Internet has affected traditional notions of sovereignty.

Readings:

Michael A. Sussman, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium*, 9 Duke J. Comp. & Int'l L. 451 (1999);

David Goldstone & Betty Shave, *International Dimensions of Crimes in Cyberspace*, 22 Fordham Int'l L.J. 1924 (1999);

Lieutenant Colonel Richard W. Aldrich, *How do you know you are at war in the information age?* 22 Hous. J.Int'l L. 223 (2000).

- N. Week 14 (April 18th): Optional review for final exam.**