

Cyber Crime Course
Course Description and Syllabus
University of Oregon School of Law
Spring Semester 2004
Adjunct Professor Sean B. Hoar
sean.hoar@usdoj.gov
541-465-6792 (voice)
541-465-6840 (fax)

I. Course Description

This two-credit course will explore the legal issues affected by on-line criminal conduct and electronic evidence. 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 electronic evidence; (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 technology of computers and the Internet; federal statutes proscribing on-line conduct; the Fourth Amendment in cyberspace; the law of electronic surveillance (including Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Electronic Communications Privacy Act, the Privacy Protection Act, and relevant provisions of the USA PATRIOT Act); and cyber crime trends, including identity theft and on-line fraud.

Given the rapid changes in technology, and the corresponding changes in crime and the law, the course will regularly include discussions of current events. There are no prerequisites, and there will be a final examination.

II. Course Summary

Of the thirteen sessions which comprise this course, the first two will discuss Internet and computer technology relevant to cyber crime. The next six 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 the following sources: 1) relevant case law and law review articles contained in this syllabus and available on-line; and 2) United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002).

III. Week-by-week Syllabus

A. **Week 1 (January 12th): Introduction to “Cyber Crime”**

The first week will serve as an introduction to the nature and scope of computer crime. The class will include a presentation on the technology of the Internet, and why it matters for the purposes of cyber crime. The class will also include a discussion of the how on-line criminal conduct should be regulated.

Readings:

Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv.L.Rev. 501 (1999);

Scott Charney, *The Internet, Law Enforcement and Security*, Internet Policy Institute (2001);

The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet; A Report of the President’s Working Group on Unlawful Conduct on the Internet, March 2000.

B. **Week 2 (January 26th): 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 electronic evidence. There will also be a demonstration of on-line investigative tools, including tracing Internet Protocol addresses. The readings will provide an introduction to the United States Sentencing Guidelines, and will lay a foundation for a discussion in Week 3 of how different conduct is treated under those guidelines.

Readings:

United States v. Debeir, 186 F.3d 561 (4th Cir. 1999);

United States v. DeMerritt, 196 F.3d 138 (2nd Cir. 1999);

United States v. Lee, 296 F.3d 792 (9th Cir. 2002);

United States Sentencing Guidelines, §§ 2A6.1, 2A6.2, 2B1.1, 2B5.3, 2G2.2. & 2G2.4.

C. **Week 3 (February 2nd) The criminalization of on-line conduct – identity theft/access device fraud**

Readings:

Federal statutes: 18 U.S.C. §§ 1028 (identity theft) & 1029 (access device fraud);

United States v. Paul, 274 F.3d 155 (5th Cir. 2001);

United States v. Sofsky, 287 F.3d 122 (2nd Cir. 2002);

Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 Or L. Rev. 1423 (2001);

United States Sentencing Guidelines § 2B1.1.

D. Week 4 (February 9th): The criminalization of on-line conduct – child pornography

Readings:

Federal statutes: 18 U.S.C. §§ 2252 & 2252A (child pornography);
United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002);
Ashcroft v. Free Speech Coalition, 535 U.S. 234, 122 S.Ct. 1389 (2002);
United States v. Mohrbacher, 182 F.3d 1041 (9th Cir. 1999);
United States v. Poehlman, 217 F.3d 692 (9th Cir. 2000);
United States Sentencing Guidelines §§ 2G2.2. & 2G2.4.

E. Week 5 (February 16th): The criminalization of on-line conduct – Internet fraud/threatening communications/interstate stalking

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);
Planned Parenthood v. American Coalition of Life Activists, 290 F.3d 1058 (9th Cir.
2002);
People v. Kochanowski, 186 Misc.2d 441, 719 N.Y.S.2d 461 (2000).
United States Sentencing Guidelines §§ 2A6.1, 2A6.2, & 2B1.1.

F. Week 6 (February 23rd): The criminalization of on-line conduct – computer fraud

Readings:

Federal statute: 18 U.S.C. §1030 (computer fraud);
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).;
United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997);
United States v. Middleton, 231 F.3d 1207 (9th Cir. 2000);
Shurgard v. Safeguard, 119 F.Supp.2d 1121 (W.D. Wash. 2000);
State v. McGraw, 480 N.E.2d 552 (Ind. 1985);
People v. Lawton, 48 Cal. App. 4th Supp. 11, 56 Cal.Rptr.2d. 521 (1996);
State v. Allen, 260 Kan. 107, 917 P.2d 848 (1996);
Newberger v. State, 641 So.2d 419 (Fla. App. 1994);
State v. Schwartz, 173 Or. App. 301, 21 P.3d 1128, *rev. denied*, 333 Or. 162, 39 P.3d 192
(2001);
Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in
Computer Misuse Statutes*, 78 N.Y.U.L.Rev. 1596 (2003).
United States Sentencing Guidelines § 2B1.1.

G. Week 7 (March 1st): The criminalization of on-line conduct – copyright infringement

Readings:

Federal statutes: 18 U.S.C. § 2319 (copyright infringement) & 17 U.S.C. § 506 (copyright infringement);

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);

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 § 2B5.3.

H. Week 8 (March 8th): The criminalization of on-line conduct – economic espionage/trade secret theft

Readings:

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

United States v. Hsu, 155 F.3d 189 (3rd Cir. 1998).

Joseph F. Savage, Jr., Matthew A. Martel, and Marc J. Zwillinger, *Conflicting Views of the Economic Espionage Act*, 15 Criminal Justice 10 (Fall, 2000).

United States Sentencing Guidelines § 2B1.1.

I. Week 9 (March 15th): Electronic evidence and the Constitution – a discussion of how the Fourth Amendment applies 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);

United States v. Bach, 310 F.3d 1063 (8th Cir. 2002);

United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (2002), Sections I & II;

J. Week 10 (March 29th): Intercepting electronic communications – a discussion of how Title III of the Omnibus Crime Control and Safe Streets Act of 1968 applies 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;

Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577 (1979);
McClelland v. McGrath, 31 F.Supp.2d 616 (N.D. Ill. 1998);
United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978);
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 Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (2002), Sections III & IV.

K. Week 11 (April 5th): Electronic Communications Privacy Act – a discussion of how the government can obtain your electronic records

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).
United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (2002), Section III & IV.

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

Readings:

Selected federal statutes pertaining to the USA PATRIOT Act;
In re Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002);
Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999).

M. Week 13 (April 19th): Sovereignty in cyber space – a discussion of how international, federal, and state relations are impacted by cyber crime

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).