

CyberCrime

Syllabus Spring 2003

Adjunct Professor Ronald N. Weikers
RNW@software-law.com

Course Times: Tuesday evenings, 5:00 to 8:00 p.m., beginning January 14, 2003

Course Description: As society becomes more dependent upon data and networks to operate our businesses, government, national defense and other critical functions, the risks posed by hacking, "malware" and cyberattacks escalate. Although cybercrimes can be analogized to more traditional criminal law violations, the technology that offenders employ is very new, making hackers more elusive and the damage they cause often more widespread. *CyberCrime* examines the new and traditional laws that govern security of data on networks, especially those that are connected to the Internet.

With good preparation, good class attendance and constructive participation, students will gain the following from *CyberCrime*: 1) An intermediate level, technical understanding of cyberattacks, networks and the Internet; 2) Knowledge of conduct that is prohibited under generally applicable security laws; and 3) An ability to critically evaluate the strengths and weaknesses of security laws and relevant caselaw. *CyberCrime* will provide students with a competitive advantage for practicing law in this cutting-edge field.

Class Format: During each class, we will discuss the assigned reading materials; a comprehensive reading list will be provided during the first class session. In addition, a portion of many classes will feature presentations made by visiting criminal prosecutors, defenders and federal agents involved in cybercrime prosecutions and investigations.

- Eligible Students:** Any post-1L student may enroll in this course. The course does not require an in-depth understanding of technical issues, but each student must at least be able to use Westlaw, prepare their final paper using Word or WordPerfect, and correspond via e-mail.
- Credits:** Three (3)
- Grading:** Grades will be based on the following components, each of which is discussed in greater detail below:
- i Class participation: ten percent (10%)
 - i A one-hour midterm examination: thirty percent (30%)
 - i A written research paper, along with an in-class presentation involving the subject matter of the research paper: sixty percent (60%)
- Class Attendance:** Franklin Pierce Law Center Academic Rules II-D ("Attendance") and II-C(6) ("Involuntary Disenrollment") will be enforced.
- Class Participation:** Ten percent (10%) of the course grade will be based on class participation. Because persuasive advocacy is an important part of every facet of the practice of law, particularly in areas that are not fully developed -- such as cybercrime --, class participation and creative thinking are encouraged. Each student will be expected to contribute to class discussions on several occasions, but quality of input is more important than quantity. The class participation portion of each student's overall grade will not be assigned anonymously.
- Midterm Examination:**
- Method:** A one (1) hour midterm examination will be administered by the registrar during the first part of the eighth class session. Answers must be legibly handwritten.
- Grading:** Thirty percent (30%) of each student's overall course grade will be based on their midterm examination score. The midterm examination will be graded on an anonymous basis.

Open Book: During the midterm examination, students may consult their own books, notes and laptops, but answers must be handwritten.

Substance: The midterm examination will consist of one (1) hypothetical fact pattern, requiring analysis of potential crimes and defenses. We will do a couple of in-class exercises that will help you to learn the format for answering the midterm examination.

Examination Tips: **Tip 1)** Follow the "IRAC" method of essay-writing (**I**ssue, **R**ule, **A**pplication and **C**onclusion). For each issue that you spot: a) Number the issue; b) Concisely identify the issue; c) Concisely state the rule of law; d) Apply relevant facts to the rule of law; and e) Posit a logical conclusion. **Tip 2)** Routine phrases and statutes may be abbreviated (e.g., "CFAA," "ECPA," "DMCA," and "NET;" these will be familiar to you very soon). **Tip 3)** If you must repeat the rule, application or conclusion discussed in your answer to an earlier issue, simply refer to your prior answer (e.g., "See Issue 1 Rule"). **Tip 4)** Read the question twice, and think about your answer, or outline it on scratch paper, for five (5) minutes before you begin to write your answer. **Tip 5)** Write neatly and in large lettering, and skip every other line, in case you need to go back and insert text.

Research Paper & Presentation:

Topic Selection: Each student's research paper and presentation will involve independent research based on a topic that directly relates to the legal issues covered by *CyberCrime*. Technical knowledge and ability are not required. Each student's proposed topic must be submitted by e-mail after the fifth class but no later than the ninth class. I must expressly approve your proposed topic via e-mail before you begin work on it, and you must promptly reply that you have received my approval. I may recommend changes, depending on whether the proposed project is appropriately challenging and/or has already been chosen by another student, and you must promptly reply.

Grading: Sixty percent (60%) of the course grade will collectively be based on the research paper and the in-class presentation. Greater weight will be given to the paper, but there is no precise formula, so excellent performance during the presentation may improve the overall score. The

research paper and in-class presentation will not be graded anonymously.

Paper Format: The paper must be approximately twenty-five typed, double-spaced pages with standard margins, using 12-point Times New Roman font. Bluebook format must be followed, and footnotes must be used for citations. Each paper must be submitted no later than 5:00 p.m. on the last examination day: 1) via e-mail in the form of a Word or WordPerfect attachment, addressed to RNW@software-law.com; and 2) in the form of two (2) printed/hard copies submitted to Ron Weikers' FPLC physical mailbox.

In-Class Presentation: Each student must give a half-hour presentation during the twelfth, thirteenth or fourteenth class session, so be prepared to go during the twelfth. Each student must also distribute a one- or two-page outline (bullet points are sufficient), so make sufficient photocopies for the entire class. You may also display a PowerPoint or similar presentation, but you must work out the technical details in advance.

Presentation Tips: Tip 1) You are not required to prepare or submit a written speech, but if you choose to draft one for your own use, keep in mind that presenters usually speak at the rate of approximately 120 words per minute. **Tip 2)** If you prepare a written speech for your own use, enlarge the font to 26-point or larger, and double-space the text. This simplifies the task of simultaneously reading and speaking. **Tip 3)** Practice your presentation at least once on your own, and again with another class member of your own choosing.

Course Materials:

Cronin and Weikers, "Data Security and Privacy Law" (West Group 2002), available at a discounted price at the Franklin Pierce bookstore. You may share this book with other students, except during the midterm examination. Other materials, such as statutes and caselaw will be required reading, and they are available for free online. The caselaw is ever-changing, so a list will be provided during the first class session, along with a list of statutes, which will likely consist of the following (listed in no particular order):

- Computer Fraud and Abuse Act, 18 U.S.C. § 1030, available at <http://www4.law.cornell.edu/uscode/18/1030.html>
- USA PATRIOT Act, H.R. 3162, 107th Cong., Pub. L. No. 107-56, 115 Stat. 272 (2001), available at <http://news.findlaw.com/cnn/docs/terrorism/hr3162.pdf>
- Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1994) (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710), available at <http://www.cpsr.org/cpsr/privacy/wiretap/ecpa86.html>
- Federal Wire Fraud Statutes, 18 U.S.C. § 1343, available at <http://www4.law.cornell.edu/uscode/18/1343.html>
- No Electronic Theft Act, Pub. L. 105-147, 111 Stat. 2678, Dec. 16, 1997, available at <http://www.techlawjournal.com/courts/elritch/pl105-147.htm> and <http://www.usdoj.gov/criminal/cybercrime/17-18red.htm> (redlined version)
- National Stolen Property Act, 18 U.S.C. § 2314, available at <http://www4.law.cornell.edu/uscode/18/2314.html>
- Economic Espionage Act, 18 U.S.C. §§ 1831-39, available at <http://www4.law.cornell.edu/uscode/18/1831.html> and <http://www.cybercrime.gov/eeapub.htm> (caselaw)
- Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. (1998) (adding §§ 512 and 1201-05 to the Copyright Act of 1976), available at http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html

First Class Assignment: Before the first class, read Chapters 1 and 2 of Cronin and Weikers, "Data Security and Privacy Law" (West Group

2002). A detailed understanding/recollection of these chapters is not required, so read them as you would read a novel. Later reading assignments involving statutes and caselaw will be shorter in length than this first assignment.

Also, before or immediately after the first class, you must send an e-mail to RNW@software-law.com and identify yourself, so that I will have all of your return e-mail addresses. All of my out-of-class communications to you will be made via e-mail, so check your in-box every day. You may occasionally communicate with me via e-mail, as well.

I look forward to working with you this semester.