Law of Computer Technology 08-532, 08-732
Prof. Shamos

Take-Home Final Exam

Exam Starts:  9:00 a.m. Tuesday, December 12, 2017
Exam Ends:  9:00 a.m. Wednesday, December 13, 2017

The purpose of this exam is to test your familiarity with legal concepts and legal reasoning involving computer technology law. It is not a test of memory or trivia. If you need access to a statute, regulation or constitutional provision, you will find it reprinted here or on the course web page. There is no need to look for statutory citations or legal cases anywhere else. If you do that, you will be wasting your time.

The exam is designed to take three hours. However, you may take as much time as you want during the 24-hour exam period. YOU MUST ANSWER ANY THREE OUT OF THE FIVE QUESTIONS. All questions are of equal weight (150 points). If you answer more than three questions, only the first three will be graded. For each question, you MUST provide an explanation for your answer. “Yes” or “No” alone, even if correct, will receive a score of ZERO. Your personal opinions about the law, how you think a situation should turn out, or what is “fair” are not relevant to this examination. You will be graded based on your ability to apply the principles learned in the course. DO NOT copy slides from the course lectures into your exam paper.

This exam is open book, open notes and open Internet. However, you may not communicate with any person during the exam about the exam or the subject matter of the course. THIS RULE CONTINUES FOR THE ENTIRE EXAM PERIOD, EVEN IF YOU HAVE HANDED IN YOUR OWN EXAM. Even though the exam is open Internet, you will not find any useful information on the Internet. When you are finished with the exam, you must submit your answers in the form of a .doc or .docx file to Canvas. There is a “Final Exam” listing under “Assignments.” DO NOT send a .pdf file. Be sure your full name is on your exam paper and is included in your filename. If you have any problem accessing Canvas, you can email the exam to shamos@cs.cmu.edu. You should retain a copy of your paper on your computer until you receive a course grade in case there is any transmission problem.

Read each question carefully before you begin answering. All the factual information you need is contained in the questions. If you believe you need additional facts to answer a question, state which facts you would need, make a reasonable assumption about them, and answer the question based on your assumption. Make sure you answer the questions that are asked. DO NOT ANSWER QUESTIONS THAT ARE NOT ON THE EXAM. Relevance counts. If you add irrelevant material to your answer in the hope of getting something right, points will be subtracted.

Please do not give anyone else access to these exam questions.
The Law of Noplacia

This exam is about a fictional place called Noplacia, which is an island off the southeastern United States. Noplacia has recently been admitted as the 51st state to the United States, is part of the U.S. legal system and is covered by the U.S. Constitution. Noplacia has adopted all of the Uniform Acts we studied in the course and the Federal Rules of Evidence as part of its state law. Noplacia is of course also subject to all federal laws and regulations. In addition to its own state courts, Noplacia has a federal district court and is within the Second Circuit for appeals purposes.

1. TAX. The Noplacia legislature is aware that other states have been having trouble collecting use tax (15 N.S. § 310, reproduced below) on goods ordered over the Internet and shipped from other states into Noplacia. It knows that it cannot force out-of-state vendors to collect Noplacia taxes, so it has passed the Noplacia Internet Sales Reporting Act, 15 N.S. § 360 (reproduced below). It requires all residents of Noplacia to install an app called TaxWatch on their personal computers and cellphones. The app uses AI to detect when a purchase has been made from an out-of-state vendor. It checks to see that the address to which the shipment is being sent is in Noplacia and whether any tax has been paid to another jurisdiction. If tax has been paid, then the Noplacia resident will receive a credit of that amount (not exceeding the Noplacia tax). The app automatically charges any remaining Noplacia use tax to the resident’s credit card. The law applies to Noplacia residents even when they are outside Noplacia. Noplacia believes that this law will vastly increase its tax revenue.

The Electronic Frontier Foundation, a non-profit organization that lobbies for digital freedom, is very concerned about this law. It brings an action against the Noplacia Tax Commissioner to enjoin enforcement of the law on the following grounds:
(i) The law invades privacy by allowing the state government to monitor all Internet activity of a resident.
(ii) The law violates the Internet Tax Freedom Act (47 U.S.C. § 151, reproduced below) because there is no reporting requirement for non-Internet sales.
(iii) If a resident orders something using a computer that is not his own, he has no way of verifying that the Tax Commissioner’s software is installed and he may not have the right to install it on a computer that is not his own.
(iv) Noplacia has no jurisdiction to force its residents to use the app when they are outside Noplacia.
(v) The law is an unreasonable burden on interstate commerce under the U.S. Supreme Court case of Quill Corp. v. North Dakota Tax Commissioner (relevant portion reproduced below).

Assume that EFF has standing to bring such a lawsuit. Explain why the EFF will either succeed or fail with EACH of its five arguments. You must explain your answers in full. A “YES” or “NO will receive ZERO credit.

2. DOMAIN NAMES. Before Noplacia became a state, a company in Noplacia called Noplacia Foods operated a chain of stores featuring the many unusual fruits, vegetables and animal products that are found only in Noplacia. When Noplacia began seeking to become a state, a Noplacia resident named Cal Clever though he might be able to make a profit. He assumed that
many companies in Noplacia would want to use domain names containing the word “Noplacia.” Cal registered 5000 such domain names, one of which was “NoplaciaFoods.com.” Cal used that domain to host 50 web pages describing Noplacia’s unusual foods and their history and nutritional value. Sure enough, when Noplacia Foods tried to register that domain, it learned that it had already been assigned to Cal Clever. Noplacia Foods had been operating under that name for over 25 years and considered the name to be its trademark. Noplacia Foods offered Cal $10,000 for the domain, but he refused the offer. Noplacia Foods then brought an administrative proceeding against Cal under the Internet Corporation for Assigned Names and Numbers (ICANN) Uniform Dispute Resolution Policy (UDRP), reproduced below. Using the tests set forth in the UDRP, determine whether Cal will get to keep the domain or whether it will be transferred to Noplacia Foods. You must explain your answer in full. A “YES” or “NO will receive ZERO credit.

3. PRIVACY. Being the newest state, Noplacia is very concerned about privacy. It has passed a comprehensive Privacy Act. One portion, 19 N.S. § 41-151.22 (reproduced below), deals with privacy of library records. Noplacia State University (NSU) is supported by public funding. Its library is highly automated and has an online catalog system accessible over the Internet but only to members of the NSU community who have university login IDs. The library collection includes many e-books. The library’s contract with publishers allows only one user at a time to access an e-book. A user can “check out” an e-book and, during the period for which it is “checked out,” that user is the only person who can access the book until it is “returned.” When it is “returned,” the original borrower no longer has access to it and it becomes available for someone else. The library catalog page for an e-book indicates whether the e-book is checked out or not. If it is checked out, the page lists the campus email address of the person who checked it out, so a person who wants it can contact that user and ask them to return it. The library website contains a link at the bottom of each page entitled “Terms of Use.” The Terms of Use page, written by Dean Easter, the head of the Library, contains the following statements: “By using the Library, you agree to these Terms of Use” and “The Library discloses the email address of any borrower of a book or e-book, but only to persons having university login IDs.”

Lena Large is a student at NSU. She is very concerned about her weight and has been checking out e-books on weight loss. When another student contacts her about returning the e-book “Half-Assed: A Weight-Loss Memoir,” she becomes very upset and goes to the police. Dean Easter is charged with a crime under 19 N.S. § 41-151.22. Lena says that the library revealed to another student that she had checked out a specific diet book and that is expressly forbidden by the statute. Easter responds by saying that (1) disclosing the email address is a reasonable way of conducting a library; (2) he had no specific personal knowledge that Lena’s email address was disclosed and criminal statutes must be construed strictly (true in Noplacia); and (3) Lena consented to the disclosure under the library’s Terms of Use. Should Easter succeed in having the charge against him dismissed? You must address all three of Easter’s defenses thoroughly. A “YES” or “NO will receive ZERO credit.

4. TRADE SECRETS. Sue Spyer works at the help desk in the IT department of Noplacia Airlines (NA). She signed a confidentiality agreement on her first day of work that prevents her from disclosing NA confidential information or using it for her own benefit. Her desktop computer is connected to her employer’s local area network, which also provides access to the
Internet. She regularly hunts around the internal airline network and one day discovers an unprotected file on the Human Resources (HR) server. This file contains the names and salaries of all NA employees, including those of the top executives. Sue’s husband, Sam Spyer, is an executive recruiter for Noplacia Placement, a private company. Sue reveals to Sam the names, titles and salaries of ten top NA executives. Sam contacts one of them to offer him a better job with a higher salary, and he accepts it and resigns from NA. NA becomes suspicious and conducts an investigation.

NA brings suit against Sue for breach of contract, violating the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (reproduced below) and the Noplacia version of the Uniform Trade Secrets Act, 22 N.S. § 101 (reproduced below). NA also brings suit against Sam for violating the Uniform Trade Secrets Act. NA contends that (a) Sue was a help desk employee not authorized to access salary records, and therefore violated 18 U.S.C. § 1030(a)(2)(C) when she obtained that information; (b) the salaries of top executives are NA confidential information which Sue improperly disclosed to Sam; (c) the salaries of top executives are a valuable trade secret, which Sue and Sam misappropriated; and (d) NA was damaged because one of its executives quit as a result of the misappropriation. Sue and Sam offer the following defenses:

(i) The Computer Fraud and Abuse Act does not apply because Sue’s computer was a help desk computer not used in interstate commerce but only internally within NA;
(ii) Even if the Computer Fraud and Abuse Act applies, Sue at all times was authorized to use her desktop computer;
(iii) NA failed to use efforts reasonable under the circumstances to maintain secrecy because it left the salary file unprotected and thus it did not qualify as either “confidential information” or a trade secret;
(iv) Sam says that salary data is not a trade secret at all because it is “readily ascertainable” by asking the employee how much he makes and it also does not have independent economic value. Furthermore, if it were really a trade secret then no employee could ever tell anyone else how much he makes without violating the law;
(v) NA was not “damaged” by the executive quitting because employees are free to quit at any time.

Evaluate each of the defenses (i)-(v) and explain carefully whether it will be successful or not. You must explain your answer in full. A “YES” or “NO will receive ZERO credit.

5. STALKING. Carol Caster is a nightly news reporter on NOTV, the main Noplacia TV station. She has been receiving hundreds of emails each week from an unknown admirer, whom we shall call Mr. Doe. The emails are not threatening, but Mr. Doe declares his love for her and begs for a face-to-face meeting. On five occasions she sent email replies asking him to please stop sending the emails, but he hasn’t stopped. Carol has received so many emails from Doe that her incoming mailbox is full and she can’t receive email from her usual friends and contacts. Doe’s email address is lover@noplace.net.

Carol sends the emails to the police and begs them to do something, citing a violation of Noplacia’s anti-stalking statute, 18 N.S. § 301.2 (reproduced below). They find that noplace.net is owned by a company in Noplacia. A detective visits the offices of noplace.net and asks for the real name of email subscriber lover@noplace.net. Noplace.net refuses to answer on the grounds
that the Stored Communications Act, 18 U.S.C. § 2702 (reproduced below) does not allow disclosure of customer records to a governmental entity. (Assume that the emails are less than 180 days old.)

The police then obtain a search warrant, raid the premises of noplace.net and learn “lover’s” identity. “He” is a 30-year-old woman living in California named Joy Netsky. Joy is indicted in Noplacia under the stalking statute. Joy has never been to Noplacia, which is 2500 miles away, owns no property there and has never done business with anyone in Noplacia, so she claims she does not have “minimum contacts” with Noplacia and it would be unconstitutional to try her there since that would “offend traditional notions of fair play and substantial justice” under the International Shoe case.

Answer ALL of the following questions:
(a) Was noplace.net legally correct in refusing to disclose the identity of lover@noplace.net? Assume that noplace.net is a “provider” under the Stored Communications Act and would be permitted to reveal the information under its announced privacy policy if it wanted to.) Explain your answer.
(b) Does Noplacia have jurisdiction to try Joy for violating the Noplacia stalking statute, 7 N.S. § 101 (reproduced below)? You must do a thorough personal jurisdictional analysis. (Subject matter jurisdiction is clear and you should not address it.)
(c) Joy’s attorney seeks to get the case dismissed, raising the defense that the stalking law, § 301.2, does not cover emails. Citing the principle of ejusdem generis, she argues that the phrase, “any other form of contact whatsoever” must be limited by the specific terms “communication while in physical proximity, telephone, mail, telegram, fax” that precede it in the statute. What these terms have in common is person-to-person speech (physical proximity or telephone) or physical pieces of paper (mail, telegram, fax), and no form of digital electronic contact of any kind is listed in the statute. Evaluate this defense.
(d) Carol sues Joy for violating the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1830 (reproduced below). Carol says that Joy exceeded authorized access to Carol’s email server because Carol told Joy to stop and caused “damage” by interfering with Carol’s access to her email because Joy’s messages filled up Carol’s mailbox. Did Joy violate the CFAA? You must explain all your answers in full. A “YES” or “NO” will receive ZERO credit.

STATUTORY REFERENCES
(In numerical order. If no number, then alphabetical)

7 N.S. § 101. Noplacia Long-Arm Statute
(a) The jurisdiction of the courts of Noplacia shall apply to the full extent permitted by the United States Constitution.

15 N.S. § 310. Use Tax
(a) A tax is hereby levied on the storage, use, or other consumption in this state of tangible personal property. The tax shall equal five (5) percent of the amount paid for such
tangible personal property. The tax shall be reduced by the amount of any tax paid to another jurisdiction for sale or use of such tangible personal property.

15 N.S. § 360. Noplacia Internet Sales Reporting Act

(a) Each resident of Noplacia who uses a computer to order any tangible goods from outside Noplacia to be shipped into Noplacia must ensure that such computer is running TaxWatch, application software provided by the Noplacia Tax Commissioner. TaxWatch shall determine the amount of any use tax due to Noplacia, giving due credit to any sales or use tax paid to any other jurisdiction, and shall cause payment of any use tax due to Noplacia to be made automatically by credit or debit card to the Noplacia Tax Commissioner.

(b) Section (a) applies to all residents of Noplacia even if they are outside Noplacia when such order is placed, and applies to all persons who are in Noplacia at the time the order is placed.

(c) Any resident of Noplacia who places an order for tangible goods to be shipped into Noplacia without using TaxWatch shall be assessed a fine of $1000 plus twice the amount of any unpaid taxes resulting from such order.

18 N.S. § 301.2. Stalking.

Anyone who repeatedly contacts another person either through communication while in physical proximity, telephone, mail, telegram, fax or any other form of contact whatsoever, regardless of the form such contact may take, and knowing such contact to be unwanted, shall be guilty of the crime of stalking, and shall be punished as provided in this Act.

18 U.S.C. § 1030. Computer Fraud and Abuse Act

(a) Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains— …

(C) information from any protected computer; …

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

shall be punished as provided in subsection (c) of this section. …
e) As used in this section—

(1) the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term “protected computer” means a computer— …

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

…

(6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

…

(8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;

…

(11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;

18 U.S.C. §2702. Stored Communications Act

(a) Prohibitions.— (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

§ 2703 (a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.

§ 2711 (4) the term “governmental entity” means a department or agency of the United States or any State or political subdivision thereof.
19 N.S. § 41-151.22. Noplacia Privacy Act (portion)

A. Except as provided in subsection B of this section, a library or library system supported by public monies shall not allow disclosure of any record or other information, including e-books, that identifies a user of library services as requesting or obtaining specific materials or services or as otherwise using the library.

B. Records may be disclosed:
   1. If necessary for the reasonable operation of the library; or
   2. On written consent of the user; or
   3. On receipt of a court order; or
   4. If required by law.

C. Any person who knowingly discloses any record or other information in violation of this section is guilty of a class 3 misdemeanor.

D. For the purposes of this section, "e-book" means a book composed in or converted to digital format for display on a computer screen or handheld device.

22 N.S. § 101. Uniform Trade Secrets Act (UTSA)

§1. Definitions
(1) "Improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.

(2) "Misappropriation " means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or

   (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason to know that it was a trade secret ad that knowledge of it had been acquired by accident or mistake.

(3) "Person" means a natural person, corporation, business trust, estate, trust, partnership, association, joint venture, government, governmental subdivision or agency, or any other legal or commercial entity.

(4) "Trade secret" means information, including a formula, pattern, compilation, program device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
§3. Damages

(a) … a complainant is entitled to recover damages for misappropriation. Damages can include both the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. In lieu of damages measured by any other methods, the damages caused by misappropriation may be measured by imposition of liability for a reasonable royalty for a misappropriator's unauthorized disclosure or use of a trade secret.

(b) If willful and malicious misappropriation exists, the court may award exemplary damages in the amount not exceeding twice any award made under subsection (a).

§4. Attorney's Fees

If (i) a claim of misappropriation is made in bad faith, (ii) a motion to terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists, the court may award reasonable attorney's fees to the prevailing party.

47 U.S.C. § 151 (note 2). Internet Tax Freedom Act

(a) Moratorium. -- No State or political subdivision thereof shall impose any of the following taxes:

(1) taxes on Internet access.

(2) multiple or discriminatory taxes on electronic commerce.

(b) Preservation of State and Local Taxing Authority. -- Except as provided in this section, nothing in this title shall be construed to modify, impair, or supersede, or authorize the modification, impairment, or superseding of, any State or local law pertaining to taxation that is otherwise permissible by or under the Constitution of the United States or other Federal law and in effect on the date of enactment of this Act.


“Due process centrally concerns the fundamental fairness of governmental activity. Thus, at the most general level, the due process nexus analysis requires that we ask whether an individual's connections with a State are substantial enough to legitimate the State's exercise of power over him. We have, therefore, often identified 'notice or fair warning' as the analytic touchstone of due process nexus analysis. In contrast, the Commerce Clause, and its nexus requirement, are informed not so much by concerns about fairness for the individual defendant as by structural concerns about the effects of state regulation on the national economy. … It is in this light that we have interpreted the negative implication of the Commerce Clause. Accordingly, we have ruled that that Clause prohibits discrimination against interstate commerce …and bars state regulations that unduly burden interstate commerce.”

Uniform Dispute Resolution Policy (ICANN)

a. Applicable Disputes. You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts … that

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

(iii) your domain name has been registered and is being used in bad faith.

In the administrative proceeding, the complainant must prove that each of these three elements are present.

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your website or other online location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your website or location or of a product or service on your website or location.

c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint. When you receive a complaint, … any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.