08-532, 08-632, 08-732 Law of Computer Technology. Prof. Shamos
Homework 1. Due Wednesday, September 28, 2016, 11:59 p.m.

Do both problems 1 and 2.

Homework policy: You may (and are encouraged to) work with other students on homework assignments provided that (1) each person’s written submission is his or hers alone; and (2) you identify on the homework each person with whom you worked in connection with the assignment. For example, you may work in pairs or groups to research, discuss and debate the homework, but then each person must go off and write their own paper. BUT: you may NEVER hand in work of another person even if you state that you have worked with that person. If you quote or paraphrase from external sources, such as web pages, you must use quotation marks to identify the quotation and identify the source of such material. Violations of these rules will be dealt with harshly to the fullest extent of University policy.

It is very useful to work in groups. Experience has shown that students produce better work when they can share ideas with colleagues. The objective of the course homework is to promote learning, not merely to serve as a grading mechanism.

Homework must be submitted as a Microsoft Word file (.doc or .docx) having a filename containing your surname by email to shamos@cmu.edu. PDF files are not acceptable because it is very difficult to add comments to them.

You must ALWAYS explain your answers. Failure to explain will result in a ZERO for the question even if your answer is correct.

You should realize that there are no “right” or “wrong” answers to these questions. The fact patterns given below are realistic but artificial and have never been decided by any court, even though they may be similar to those of actual cases. You will not find these scenarios on the Internet. They were constructed for the purposes of this homework. However, the legal citations and statutes are real. The fact that a court may have decided a similar case in a particular way does not make that decision the “right” answer. Your grade will depend on the degree to which you follow the methods taught in the course for analyzing cases of this type.

These problems require thought. You will need to decide which facts are relevant and which are not. DO NOT use your personal sense of justice to decide which way the cases should turn out. You MUST apply the principles of legal reasoning discussed in the course. You will find it impossible to write effective answers to these questions if you wait until the last night before the homework is due. Your answers do not need to be long but they should be thorough.

If you find that there is some factual information you need that is not stated in the question, then make a reasonable assumption about that information and state and justify your assumption.
1. Interpreting Statutes [60 points].

Peter Printer, a resident of the state of California, is very clever. He has designed some malware called FINGR that invades an iPhone and does several things: it (1) captures a digitized version of the user’s fingerprint as recorded by TouchID, the iPhone’s fingerprint sensor; (2) sends the digitized fingerprint, phone number and the iPhone’s IP address to a cloud server; and (3) accepts a digitized fingerprint over the Internet as long as it matches the user’s TouchID fingerprint and allows remote access to apps that normally require fingerprint authorization. FINGR is obviously a powerful way of obtaining information from a phone.

Peter Printer offers a free cellphone game that installs FINGR on any iPhone to which the game is downloaded. Pam Private, a resident of the state of Georgia, downloads the game and, without her knowledge, FINGR is now on her iPhone. Each time she uses TouchID, FINGR uploads her digital fingerprint and IP address to Peter’s cloud. The same is true for every other user of the game.

Printer now offers customers the ability to penetrate iPhones. He sells an app called WATCHIT. Given a cellphone number, WATCHIT accesses Peter’s cloud, obtains the phone’s IP address and the user’s fingerprint and is able to invoke any app remotely that requires a fingerprint. The price of WATCHIT is $1000 for each person whose iPhone is accessed.

Sam Sneaker, who is Pam’s boyfriend and a resident of Florida, pays Peter $1000 for WATCHIT and submits Pam’s cell number to Peter’s server. This gives Sam access to Pam’s fingerprint-protected apps. Sam suspects that Pam is seeing another man and he wants to view her email, which is fingerprint-protected. Using WATCHIT, Sam is easily able to read all of Pam’s emails and he discovers that Pam has been having an intimate relationship with Hugh Handsome, a resident of Alabama. Sam confronts Pam, explains how he got access to the email, and ends their relationship.

Pam is horrified that her phone has been compromised, so she takes it to a security expert to have WATCHIT removed. The expert charges $750 for this service, but explains that he cannot be sure that he removed everything and recommends that, to be safe, Pam should get another iPhone. She buys an iPhone 6 for $399.

Pam goes to the police and tells her story. The police question Sam and learn about Peter. Sam and Peter are arrested by the police in their states and delivered to Georgia. Sam is prosecuted for “Computer Invasion of Privacy” under the Official Code of Georgia Annotated (O.C.G.A) § 16-9-93(c) (reproduced below). Peter is prosecuted for “Computer Password Disclosure” under O.C.G.A. 16-9-93(e) (reproduced below).

Sam’s lawyer argues that emails between lovers do not contain any “employment, medical, salary, or credit” data and therefore do not qualify as “any other financial or personal data” under § 16-9-93(c). He asks the Court to dismiss the charges against Sam.

Peter’s lawyer argues that a fingerprint does not qualify as a password under § 16-9-93(e). A fingerprint is not a “number, code or password” and therefore is not an “other means of
access to a computer.” Peter agrees that an iPhone is a “computer” for purposes of the statute, but challenges the charge that he disclosed a password. Peter also says that he did not disclose anything – the transfer of the fingerprint was all done by software. Peter’s lawyer also says that Pam did not suffer any “victim expenditure” in excess of $500 because she did not spend money to “verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.” He argues that removing the malware was not “verifying” anything and that buying a new iPhone was also not “verifying” anything. He asks the Court to dismiss the case against Peter.

In Georgia, a criminal statute is “strictly construed,” which means, as expressed by the Georgia Supreme Court, it “must be construed strictly against criminal liability and, if it is susceptible to more than one reasonable interpretation, the interpretation most favorable to the party facing criminal liability must be adopted.” In question 1, DO NOT CONSIDER SUBJECT MATTER OR PERSONAL JURISDICTION. ASSUME THAT GEORGIA HAS SUBJECT MATTER JURISDICTION AND ALSO HAS PERSONAL JURISDICTION OVER SAM AND PETER.

QUESTION 1a: SHOULD THE COURT DISMISS THE CASE AGAINST SAM BECAUSE THE STATUTE DOES NOT APPLY TO SAM’S ACTIONS? You must answer this question based on the legal principles learned in the course, not on your personal feeling about what the result should be. You must address the arguments made by Sam’s lawyer. The fact that Sam may have committed other crimes is irrelevant. You are only to consider the one crime he is charged with under § 16-9-93(c).

QUESTION 1b: SHOULD THE COURT DISMISS THE CASE AGAINST PETER BECAUSE THE STATUTE DOES NOT APPLY TO PETER’S ACTIONS? You must address the arguments made by Peter’s lawyer. The fact that Peter may have committed other crimes is irrelevant. You are only to consider the one crime he is charged with under § 16-9-93(e).

Computer crimes defined

(c) Computer Invasion of Privacy. Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy. “Data” includes any representation of information, intelligence, or data in any fixed medium, including documentation, computer printouts, magnetic storage media, punched cards, storage in a computer, or transmission by a computer network.

(e) Computer Password Disclosure. Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of
the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.

…

(g) Civil Relief; Damages.
(1) Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, “damages” shall include loss of profits and victim expenditure. “Victim expenditure” means any expenditure reasonably and necessarily incurred by the owner to verify that a computer, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by unauthorized use.

…

(3) The provisions of this article shall not be construed to limit any person’s right to pursue any additional civil remedy otherwise allowed by law.

(h) Criminal Penalties.
(1) Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than $50,000.00 or imprisoned not more than 15 years, or both.
(2) Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.

2. Interstate Jurisdiction [60 points].

Assume all the same facts as in Question 1. However, the answer to this Question 2 does not depend on whether the criminal cases against Sam and Peter were dismissed. The answer to Question 2 is independent of the answer to Question 1.

Pat Private brings a civil lawsuit against Sam Sneaker in Georgia under O.C.G.A. § 16-9-93(g). She claims that his violation of her privacy under § 16-9-93(c) caused her to suffer damages. In particular, her most intimate conversations with Hugh Handsome were exposed to Sam, for which she seeks $1 million in compensation for violation of privacy and embarrassment.

Pat Private brings a different civil lawsuit against Peter Printer in Georgia under O.C.G.A. § 16-9-93(g). She claims that his violation of § 16-9-93(e) caused her to suffer damages. In particular, because of Peter’s software, she suffered great emotional distress worrying about who else might have had access to her private communications. She asks for $500,000 in damages plus all of the costs associated with examining and replacing her iPhone.

Sam’s attorney argues that Sam is not a resident of Georgia and the courts of Georgia do not have personal jurisdiction over Sam. While Sam has visited Pam in Georgia at least 20 times, none of those visits had anything to do with the alleged violation of privacy. Sam owns a boat, which he keeps in a marina in Georgia, but it is located 100 miles away
from Pam’s house. Sam kept a toothbrush and some clothing at Pam’s house, but does not own any other property in Georgia.

Peter’s attorney argues that Peter is not a resident of Georgia and the courts of Georgia have no personal jurisdiction over Peter, who has never been to Georgia. Peter knew that Sam was in Florida, but had no knowledge that Sam would use the fingerprint to access any information about a Georgia resident, did not know and could not have known that Sam would use Pam’s fingerprint, and that Peter never heard of Pam and did not know she was in Georgia. Peter owns no property in Georgia and has no employees in Georgia. Peter has sold a total of 900 copies of WATCHIT all over the world, and 30 of them were to residents of Georgia, which Peter delivered over the Internet, but Peter’s copy (to Florida) was not one of the 30.

Assume that the jurisdictional facts alleged by Sam and Peter are accurate and that Pam does not contest them.

QUESTION 2a: SHOULD THE COURT DISMISS THE CASE AGAINST SAM FOR LACK OF PERSONAL JURISDICTION? You must address each of the arguments made by Sam’s lawyer.

QUESTION 2b: SHOULD THE COURT DISMISS THE CASE AGAINST PETER FOR LACK OF PERSONAL JURISDICTION? You must address each of the arguments made by Peter’s lawyer.

NOTE: QUESTION 2 IS ALL ABOUT JURISDICTION IN CIVIL (NOT CRIMINAL) CASES. DO NOT ASSUME THAT GEORGIA HAS PERSONAL JURISDICTION OVER SAM AND PETER. THAT IS WHAT YOU ARE TO ANALYZE. YOU MUST CONSIDER THE GEORGIA LONG-ARM STATUTE, REPRODUCED BELOW.

Georgia Long-Arm Statute

§ 9-10-91. Grounds for exercise of personal jurisdiction over nonresident
A court of this state may exercise personal jurisdiction over any nonresident … as to a cause of action arising from any of the acts, omissions, ownership, use, or possession enumerated in this Code section, in the same manner as if he were a resident of the state, if in person or through an agent, he:
(1) Transacts any business within this state;
(2) Commits a tortious act or omission within this state, except as to a cause of action for defamation of character arising from the act;
(3) Commits a tortious injury in this state caused by an act or omission outside this state if the tort-feasor regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered in this state;
(4) Owns, uses, or possesses any real property situated within this state; or