Chapter 2

_____ In *Olmsted v. United States* (1928), the U.S. Supreme Court interpreted the Fourth Amendment to apply only to physical intrusion. **(T)**

_____ In *Katz v. United States* (1967), the U.S. Supreme Court determined that the government needs a court order to intrude where a reasonable person has a reasonable expectation of privacy. **(T)**

_____ The Omnibus Crime Control and Safe Streets (1968) explicitly allowed wiretapping and electronic surveillance by law enforcement agencies with a warrant. **(T)**

_____ The USA PATRIOT Act (2001) gives individuals more protection from governmental intrusion. **(F)**

_____ In *Kyllo v. United States* (2001), the U.S. Supreme Court ruled that when the government uses a device that's not in use by the general public to "see" things it could not without intrusion, that is a "search" and requires a warrant. **(T)**

_____ *U.S. v. Jones* (2012) was the first major case of digital technology surveillance and involved police attaching a GPS tracking device to a person's vehicle without a search warrant. **(T)**

Chapter 2

1. Two approaches to the problem of protecting personal information are (a) the free market view and (b) the consumer protection view. How do these points of view differ on the issue of a company disclosing personal information about its customers? How do they differ on the issue of errors in the data about an individual that is distributed by a credit bureau?
2. Briefly describe what an "opt-in" policy is and an "opt-out" policy is. Let's say you were filling out a survey for an online magazine. Give an example of what you'd see that would distinguish an opt-in from an opt-out policy.
3. Consider the European Union and the United States. Which one of these cultures has historically placed a higher value upon privacy? Explain.
4. Why did the United States try to restrict strong encryption? What effect did that attempt at restriction have on U.S. businesses?
5. What are some "pros" and "cons" to having a national ID card that can access all of one's financial and medical information?

6. Would the Social Security Number be good to use as a national ID for U.S. citizens? Why or why not?

Chapter 2

1. When a person visits a Web site, his or her IP address and the links he or she clicked on are automatically recorded. This is an example of

   (a) secondary use

   (b) invisible information gathering

   (c) data spillage

   (d) data mining

Correct answer: b - pg 56-57

2. The Privacy Act of 1974 established rules to regulate

   (a) private sector databases only

   (b) all databases that contain personal information

   (c) all personal information, including surveillance data

   (d) Federal government databases only

Correct answer: d - pg 84

3. A cookie is

   (a) a feature of a Web site designed to attract children

   (b) an illegal use of information about a customer

   (c) a file that a Web site stores on a visitor's computer

   (d) a small reward that can be redeemed on a Web site

Correct answer: c - pg 58

4. If a business follows an "opt-in" policy for handling personal data, information about a customer

   (a) may not be released under any conditions

   (b) may not be released unless the customer gives permission

   (c) may be released unless the customer requests that the information be kept private

   (d) may be released for any legitimate business purpose

Correct answer: b - pg 59

5. The Communications Assistance for Law Enforcement Act (CALEA) said that

   (a) international electronic communications must be filtered through a single hub.

   (b) agents of a foreign power may be wiretapped with authorization from a secret court

   (c) telecommunications equipment must be designed to allow the interception of telephone calls (with a court order)

   (d) email should have the same degree of legal protection as telephone calls

Correct answer: c - pg 115

Chapter 2

FISA	the Act which establishes oversight rules for the NSA
FTC	the federal commission that regulates trade
FCC	the federal commission that regulates communications
computer matching	combining and comparing information from different databases using a single identifier
targeted marketing	advertising based on demographics, purchasing history, or other specific aspects of people
COPPA	a law passed to protect children's privacy online
data mining	combing through large amounts of data for patterns and information
computer profiling	analyzing data to determine characteristics of people most likely to engage in a certain behavior
RFID	tags that use radio frequencies to communicate with devices
CALEA	the law that requires communications companies to design equipment so that it is capable of being tapped
GPS	uses satellite signals and triangulation to determine location
encryption	a technology that transforms data into a form that is meaningless to anyone who might intercept it
ECPA	a law which prohibits interception of email and reading of (some) stored email without a court order

Chapter 2

1. Explain why the United States has historically placed less value than the European Union on the right to privacy.

2. Describe three of the Fair Information Principles.