

2 Privacy

Objectives

After completing this chapter, the student should be able to:

- Understand how privacy is threatened by technology;
- Describe the key sources of privacy law;
- Understand the elements of the four main privacy torts; and
- Describe the major federal laws in the United States that affect personal privacy.

“Wherever the real power in a Government lies, there is the danger of oppression. In our Governments, the real power lies in the majority of the Community, and the invasion of private rights is chiefly to be apprehended, not from the acts of Government contrary to the sense of its constituents, but from acts in which the Government is the mere instrument of the major number of the constituents.”

James Madison, Letters and Other Writings of James Madison Volume 3

2.1 Introduction

Privacy is often defined as the “right to be left alone.”²⁰ From a legal perspective, the right to privacy involves control over one’s personal information, such as name, address, birthdate, health data, assets, and certain types of privileged communications.²¹

In *The Right to Privacy*,²² authors Ellen Alderman and Caroline Kennedy noted “the word ‘privacy’ does not appear in the United States Constitution. Yet ask anyone and they will tell you they have a fundamental right to privacy. They will also tell you that privacy is under siege.”²³

That siege is most evident with the Internet, as it presents one of the greatest threats to personal information and privacy.

2.2 Threats to Privacy

Threats and challenges to privacy existed before the Internet, even when paper was the standard medium for saving personal and business information. However, as technology and the Internet have developed, personal information is saved on all types of devices including computers, cell phones, tablets, and even activity bands such as Jawbone® and Fitbit®.

Two main areas threaten a person’s privacy. The first involves other people. The second threat is from the government (both state and federal). In the United States, governmental privacy issues are concentrated at the federal level.



Figure 2-1 Used with permission

2.3 Sources of Privacy Law

US privacy law is based on five specific areas: 1) the **U.S. Constitution and Amendments**, 2) **state constitutions**, 3) **common law torts**, 4) **federal and state statutes**, and 5) **administrative agency rules and actions**.

2.4 U.S. Constitution and Amendments

The right to privacy is not expressly stated in the US Constitution or its Amendments; however, the right to privacy has been recognized by American courts²⁴ as a **derived** or **implied** right. A derived right is one inferred through Constitutional language.

The U.S. Supreme Court has stated the right of privacy is a derived right through three Amendments: the **Fourth**, **Fifth** and the **Ninth**. These three Amendments protect individuals against an invasion of privacy by the federal *government*. This protection does not extend to personal privacy disputes.

Fourth Amendment	Fifth Amendment	Ninth Amendment
<p>“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”</p>	<p>“No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”</p>	<p>“The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”</p>

Figure 2-2

The *Fourth Amendment* guarantees that individuals will not be subject to unreasonable searches and seizures by the federal government. The key language involving privacy in this Amendment is “the right of the people to be secure in their persons, houses, papers, and effects...”

Maastricht University *Leading in Learning!*

Join the best at the Maastricht University School of Business and Economics!

Top master's programmes

- 33rd place Financial Times worldwide ranking: MSc International Business
- 1st place: MSc International Business
- 1st place: MSc Financial Economics
- 2nd place: MSc Management of Learning
- 2nd place: MSc Economics
- 2nd place: MSc Econometrics and Operations Research
- 2nd place: MSc Global Supply Chain Management and Change

Sources: Keuzegids Master ranking 2013; Elsevier 'Beste Studies' ranking 2012; Financial Times Global Masters in Management ranking 2012

Visit us and find out why we are the best!
Master's Open Day: 22 February 2014

Maastricht University is the best specialist university in the Netherlands (Elsevier)

www.mastersopenday.nl

The U.S. Supreme Court decided its first landmark privacy case interpreting the Fourth Amendment in 1965 in *Griswold v. Connecticut*.²⁵ In *Griswold*, a married couple sued the State of Connecticut for a violation of their marital privacy. At that time, it was a state crime for a married couple to use any form of birth control. The Court found the law unconstitutional, recognized marital privacy in the bedroom, and established “zones of privacy,” or areas or locations that were protected from government intrusion.²⁶

As the law evolved, so did the zone of privacy. Later court cases held, if a person has an expectation of privacy and society recognizes the expectation as reasonable, then the privacy zone might expand. For example, it is reasonable to expect that a public restroom will not include cameras or other recording devices.

The *Fifth Amendment* stands for the proposition that no person shall be compelled to be a witness against him or herself. The familiar phrase that “you have a right to remain silent,” comes from the Fifth Amendment. Corporations do not have this protection.

The last two Amendments that deal with privacy are the *Ninth* and *Fourteenth*. The Ninth Amendment states “[t]his enumeration shall not be construed to deny other rights retained by the people...” The reading of the Amendment is somewhat fuzzy, but the U.S. Supreme Court has broadly interpreted the Ninth Amendment to infer privacy protection in ways not detailed in the first eight Amendments. This implies there are additional privacy rights not mentioned in the other Amendments.

The Fourteenth Amendment gives individuals privacy protection from *state* governments using the federal constitutional standards.

This leads us to several growing questions. For example, is it a violation of privacy for the federal government to monitor a person’s computer usage or cell phone conversations? How private are someone’s files saved in the cloud? What are the privacy issues with wearable technology (such as Google Glass™) that can record and take photos? Alternatively, how can an individual’s privacy be protected as new technologies are created?

2.5 State Constitutions

The second source of privacy law involves state constitutions. It is common for a state to include the language of the federal Fourth Amendment in its constitution, and protect individuals from a **state government’s** invasion of privacy. However, many state constitutions *go further* and protect an individual’s privacy from the government in other areas, such as medical records, wiretapping, insurance information, school documents, credit data, financial information, and privileged communications (*i.e.*, attorney-client or physician-patient).

2.6 Common Law Torts

The third source of privacy law is **common law**²⁷ torts.

A tort is a wrong of one person against another. Torts are not crimes. Instead, they involve civil disputes that often result in litigation. A tort must have some sort of quantifiable damages for recovery.

There are four main categories of privacy torts:

1. **Intrusion upon seclusion** (often called intrusion);
2. **Public disclosure of private facts** that causing injury to one's reputation;
3. Publicly placing a person in a **false light**; and
4. **Misappropriation** of a person's name or likeness.



Figure 2-3 Used with permission

2.6.1 Intrusion

Intrusion upon seclusion (also called intrusion) is defined as “intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.”²⁸

Three elements must be present for intrusion to take place:

1. There must be an intent to intrude or the knowledge the intrusion was a violation;
2. The person being violated must have had a reasonable expectation of privacy; and
3. The intrusion must be substantial and highly offensive to a reasonable person.

Publication such as posting on the Internet is not a required element.

People in public places have little expectation of privacy. People engaging in public activities must assume they might be photographed or filmed, or that what they say publicly might be recorded.

Photographing or recording another person may constitute an intrusion upon seclusion. Photographing a couple kissing in a public venue would not invade their privacy, but photographing them in a hotel room would. The difference is the expectation of privacy: public versus private.

Defenses to the claim of intrusion include:

- That you did not enter the person's private property;
- That the person gave you consent to enter their property;
- That it is **custom and usage** that privacy is waived. This means, for example, if it is standard practice for a medic to respond to an emergency fire call and the medic enters a person's home, a person could not allege intrusion if the homeowner did not expect the medic to accompany the fire department into the house.

Although property is being used here in the traditional sense (*i.e.*, real estate), courts have expanded this tort to include **electronic property rights**.²⁹



The advertisement features a portrait of a young woman with red hair on the left side. On the right side, there is a white diagonal area containing the following text: a blue right-pointing chevron followed by "Apply now" in bold blue font; "REDEFINE YOUR FUTURE" in blue; "AXA GLOBAL GRADUATE PROGRAM 2015" in bold blue; the "redefining / standards" logo in blue and red; and the AXA logo in blue and white. A small vertical watermark "agence.cdg. © Photomostop" is visible on the left edge of the image.

2.6.2 Public Disclosure of Private Facts

Public disclosure of private facts causing injury to reputation is defined as publicly disclosing or transmitting highly private or personal information about another that causes damage to their reputation. The private facts made public must be personally embarrassing facts. The information must be “highly offensive to a reasonable person of ordinary sensibilities.”³⁰

The elements that must be proven for this tort include:

1. An intent to communicate the facts;
2. The disclosure must be highly offensive to a reasonable person;
3. The facts disclosed must be private or personal; and
4. The information must be communicated or publicized to a significant segment of the community.

Examples of Private Facts
<ul style="list-style-type: none">• Information on a person’s medical condition (such as positive for HIV) posted on Facebook®• Someone’s sexual history posted on a blog• A viral video showing a person engaging in illegal drug use

Figure 2-4

Defenses to the claim include:

- The information was newsworthy;
- The party consented to the disclosure of the information;
- There existed a *qualified privilege*;³¹
- The information did not outrage the community’s notion of decency;
- The event took place in public; or
- The information was a matter of public record.

2.6.3 Publicly Placing Another in a False Light

Publicly placing another in a false light means “falsely connecting a person to an immoral, illegal, or embarrassing situation causing damage to their reputation.”³²

There are two elements involved with a false light claim. First, it must be shown that “the false light would be highly offensive to a **reasonable person**,” and second, that “the person committing the action had knowledge of, or acted in reckless disregard as to the falsity of the publicized matter, and the false light in which the other would be placed.”³³

The *reasonable person standard* is often used in defining a wrong. It simply means the actions of the defendant is distasteful to the average person and to society in general.

False light publicity includes incorrectly attributing an opinion or statement to another person, suing someone and using his or her name without authorization, or using another person's name on a petition without approval. This would include statements posted on the Internet, text messages, tweets, *etc.*

Some defenses to this tort would be:

- The individual was not identified;
- The information came from a privileged source;
- The information was not offensive to a reasonable person; and
- A person consented.

False light and the tort of defamation are often confused. Remember that false light involves hurting a person emotionally by embarrassing them. Defamation is an intentional false communication, either written (libel) or spoken (slander) that harms a person's reputation (see Chapter Five). To prove false light the information must be "highly offensive to a reasonable person." To prove defamation, the information must "adversely harm a person's reputation." Therefore, the threshold of proof is lower for defamation.

Truth is not generally a defense to false light lawsuits, whereas truth is a defense in defamation lawsuits.

2.6.4 Misappropriation of a Person's Name or Likeness

Misappropriation (often called appropriation) is defined as using the name, likeness, or identity of a living person, without their permission or consent, **for commercial gain or advantage**. For example, an advertising company uses a celebrity's likeness or identity to sell a client's product. If the celebrity did not consent to the use of their photo to endorse the merchandise, then a claim of misappropriation might exist.

An example of misappropriation occurred in 2010 involving President Obama and the outerwear company Weatherproof®. The company created a billboard ad using a photo of the President showing President Obama standing in front of the Great Wall in China wearing one of Waterproof's coats. The tagline of the ad said "A Leader in Style." The company was asked by the White House to remove the billboard. The official White House response was "[i]t is misleading and suggests approval by the President or the White House, and the White House has a long-standing policy not allowing a President's name and likeness to be used for commercial purposes."³⁴

2.6.4.1 Limitations

A limitation on the tort of misappropriation occurs when there is no actual confusion. Consider voice misappropriation, for example. When a comedian imitates celebrities' voices, everyone recognizes the imitation and no one is confused about the speaker's identity. If there is no confusion, then there is no appropriated interest of the plaintiff.



Figure 2-5 Used with permission

**Empowering People.
Improving Business.**

BI Norwegian Business School is one of Europe's largest business schools welcoming more than 20,000 students. Our programmes provide a stimulating and multi-cultural learning environment with an international outlook ultimately providing students with professional skills to meet the increasing needs of businesses.

BI offers four different two-year, full-time Master of Science (MSc) programmes that are taught entirely in English and have been designed to provide professional skills to meet the increasing need of businesses. The MSc programmes provide a stimulating and multi-cultural learning environment to give you the best platform to launch into your career.

- MSc in Business
- MSc in Financial Economics
- MSc in Strategic Marketing Management
- MSc in Leadership and Organisational Psychology

BI NORWEGIAN BUSINESS SCHOOL

EFMD
EQUIS
ACCREDITED

www.bi.edu/master



Defenses to the claim of appropriation include:

- Newsworthiness;
- Consent; or
- The individual was not identified.

In most states, there are also different standards for a private person and someone in the public light (such as a celebrity). For example, a superstar could receive damages for the unauthorized use of their likeness, because the associated likeness has monetary value.

2.6.4.2 Examples

Meet Bobby B. and three different fact situations.

Scenario 1. Bobby B. is known as a straight shooter. However, one day Bobby drank excessively at a Pittsburgh Pirates baseball game at a company outing on company time and sponsored by his employer. Bobby was not known for being a heavy drinker, so the news spread quickly at work about his drunken behavior. The drinking took place in a public venue; hence, there was no expectation of privacy.

Scenario 2. Assume that Bobby B. got drunk at a bar in a red light district while vacationing overseas. Bobby B. tells his best friend Raymondo about his escapades. Raymondo makes a post on Ello™ about Bobby's drunken escapades. Bobby's behavior took place in a public venue; hence, there was no expectation of privacy.

Scenario 3. After a hard day at work, Bobby B. has one too many drinks while sitting alone in his backyard. His backyard is fenced in, and he cannot be seen unless someone intentionally peers over the fence. His nosy neighbor Jo peeks over the fence, observes Bobby B. drinking heavily, takes photos of Bobby with the empty beer bottles, and shares the pictures with everyone on the block. Is this a private or public venue? Is there an expectation of privacy in your fenced backyard? Many would say yes.

When you look at these factual situations, you will see that privacy is based on your physical location, whether the situation involved a private activity, and whether others were present. In addition, the privacy limits are clear. What if in scenario 2, a friend took a photo of Bobby B. in the bar and posted the photo on the Internet? Alternatively, what if Bobby B. posted a tweet describing his intoxicated state? What if, in Scenario 3, Bobby B. posted a private message on Facebook about his drinking, and posted a selfie with a drink in his hand? What if a friend posts the photo on a public blog? Yes, all the rules must be rewritten in a 24/7 technological world.

2.7 Federal and State Laws

Both federal and state laws protect an individual's privacy rights. Because each state will have its own set of privacy laws, this section will focus on key federal legislation in the privacy area.

Download free eBooks at bookboon.com

As you learn and read about federal privacy laws, it will be clear that Congress has not stayed current with the changes in technology. This inaction makes it more difficult for current laws to be effective.

Federal laws (also called statutes), are located in a set of books called the **U.S. Code** (also known as the U.S.C.). They are categorized and organized into groupings called **titles** (e.g., Title 47). Each title represents a specific subject. The laws are further broken down into groups called **sections**. Often you will see the section symbol §, used to introduce the section of a federal law. For example, 47 U.S.C. § 551 means the law is located in Section 551 of Title 47 in the United States Code.

The following laws address significant privacy issues. Each will be discussed further in this chapter. They include:

- Cable Communications Policy Act of 1984 – 47 U.S.C. § 521
- CAN-Spam Act of 2003 – 15 U.S.C. § 103
- Children’s Online Privacy Protection Act of 1998 – 5 U.S.C. § 6501
- Computer Fraud and Abuse Act of 1986 – 18 U.S.C. § 1030
- Currency and Foreign Transactions Act of 1970 – 31 U.S.C. § 5311
- Electronic Communications Privacy Act of 1986 – 18 U.S.C. § 2510
- Fair Credit Reporting Act of 1970 – 15 U.S.C. § 1681
- Family Educations Rights and Privacy Act – 20 U.S.C. § 1232g
- Freedom of Information Act – 5 U.S.C. § 552
- Gramm-Leach-Bliley Act of 1999 – 15 U.S.C. § 6801
- Health Insurance Portability and Accountability Act of 1996 – 42 U.S.C. § 300gg and 29 U.S.C § 1181 and 42 U.S.C. 1320d
- Privacy Act of 1974 – 5 U.S.C. § 552a
- Privacy Protection Act of 1980 – 42 U.S.C. § 2000aa
- Right to Financial Privacy Act of 1978 – 12 U.S.C. § 3401
- Telephone Consumer Protection Act of 1991 – 47 U.S.C. § 227
- Video Privacy Protection Act of 1988 – 18 U.S.C. § 2710
- USA Patriot Act³⁵ (various)

2.7.1 Cable Communications Policy Act of 1984³⁶

Damages Available for Cable Communications Policy Act Violations³⁷
<ul style="list-style-type: none">• A monetary amount equal to the amount the subscriber has been damaged;• The amount awarded can be no less than the higher of \$1000 or \$100 a day for each day the law has been violated;• Punitive damages;• Reasonable attorney fees; and• Court costs.

Figure 2-6

The Cable Communications Policy Act of 1984 is a law that created a “national policy concerning cable communications.”³⁸ A portion of the law included language to protect the privacy rights of cable subscribers.

Three major privacy requirements are included in the law. First, cable companies cannot reveal individual viewing preferences without the consent of the subscriber. Second, the law required cable companies to provide subscribers with a written notice about the company’s privacy practices and its process for collecting and distributing “personally identifiable information.” Last, the law required cable operators to provide this notice yearly. Civil monetary damages are available for a breach of privacy as detailed in Figure 2-6.

2.7.2 CAN-SPAM Act of 2003³⁹

Spam is the sending of an unsolicited email advertisement. The CAN-SPAM Act of 2003 prohibits deceptive practices in these types of emails. The law “bans false or misleading header information.” In addition, subject lines must be truthful, and the email must be identified as an advertisement. The email must also include instructions how to opt out of future emails, and include a “valid physical postal address” in the message.⁴⁰

Need help with your dissertation?

Get in-depth feedback & advice from experts in your topic area. Find out what you can do to improve the quality of your dissertation!

Get Help Now



Go to www.helpmyassignment.co.uk for more info



Helpmyassignment



Example of a CAN-SPAM Act of 2003 Compliant Email

2 Free Stainless Steel Coffee Tumblers

▼ Sent By: "Seattle Coffee" <rester@wardots.info> On: Feb 02/21/09 4:24 AM

To: Konnie Kustron
Reply to: service@wardots.info



SeattleCoffeeDirect.com

5 for \$5 each

Act now and get 2 new Stainless Steel Coffee Tumblers, 1 set of new 14 oz. Coffee Mugs and 2 Gourmet Bags of Coffee + **Free Shipping!**

[CLICK HERE FOR DETAILS](#)

Satisfaction Guaranteed
No Obligation

BRAZILIAN SANTOS

Gourmet House Blend

Sumatra Mandheling

Costa Rica Tres Rios

Hawaiian Hazelnut

Guatemala Antigua

If you have decided you would no longer like to receive mailings from Seattle Coffee Direct, please [visit here](#) or mail us at 990 grove St. Ste 204, Evanston, IL 60201

This is an Advertisement. Your email address has been verified to receive offers from one of our affiliates. We respect your privacy and pledge not to abuse your email address. If you prefer not to receive further emails of this type please "[CLICK HERE TO BE REMOVED](#)". Your Request WILL be honored.

*Or write to PO Box 17598 #88657 Baltimore, Maryland 21297-1598
Your removal request will be honored.
This ad is in full compliance with US Federal CAN-SPAM act 2003*



Figure 2-7 Used with permission

CAN-SPAM Act – A Compliance Guide for Business⁴¹

Despite its name, the CAN-SPAM Act doesn't apply just to bulk email. It covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," including email that promotes content on commercial websites. The law makes no exception for business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law.

Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to \$16,000, so non-compliance can be costly. But following the law isn't complicated. Here's a rundown of CAN-SPAM's main requirements:

1. **Don't use false or misleading header information.** Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
2. **Don't use deceptive subject lines.** The subject line must accurately reflect the content of the message.
3. **Identify the message as an ad.** The law gives you a lot of leeway in how to do this, but you must disclose clearly and conspicuously that your message is an advertisement.
4. **Tell recipients where you're located.** Your message must include your valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've registered with a commercial mail receiving agency established under Postal Service regulations.
5. **Tell recipients how to opt out of receiving future email from you.** Your message must include a clear and conspicuous explanation of how the recipient can opt out of getting email from you in the future. Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. Give a return email address or another easy Internet-based way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you. Make sure your spam filter doesn't block these opt-out requests.
6. **Honor opt-out requests promptly.** Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient's opt-out request within 10 business days. You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the CAN-SPAM Act.
7. **Monitor what others are doing on your behalf.** The law makes clear that even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible.

Figure: 2-8

2.7.3 Children's Online Privacy Protection Act of 1998⁴²

The Children's Online Privacy Protection Act of 1998 (COPPA) prohibits the online collection of personal information about children under age 13 without parental consent.⁴³

The law applies to operators of commercial sites targeted to (or those who knowingly collect information from) children under 13. COPPA requires these sites to have a "prominent statement link on their home page" to the website's privacy practices. The law also requires the vendor to obtain verifiable parental consent before collecting personally identifiable information from children. Enforcement of the law is through the Federal Trade Commission (FTC) and Attorney General's office for each state.

An example of protection under COPPA occurred in the 2002 case filed by the FTC against the Ohio Art Company, the makers of the well-known drawing toy Etch-A-Sketch toy. Specifically the FTC alleged that the Ohio Art Company:

...collected the names, mailing addresses, e-mail addresses, age, and date of birth from children who wanted to qualify to win an Etch-A-Sketch toy on their birthday. The FTC charged that the company merely directed children to “get your parent or guardian’s permission first,” and then collected the information without first obtaining parental consent as required by the law. In addition, the FTC alleged that the company collected more information from children than was reasonably necessary for children to participate in the “birthday club” activity, and that the site’s privacy policy statement did not clearly or completely disclose all of its information collection practices or make certain disclosures required by COPPA. The site also failed to provide parents the opportunity to review the personal information collected from their children and to inform them of their ability to prevent the further collection and use of this information, the FTC alleged.⁴⁴

The lawsuit, filed in the U.S. District Court for the Northern Ohio, resulted in a settlement.⁴⁵ The Ohio Art Company agreed to pay the Federal Trade Commission \$35,000 for violating COPPA by collecting personal information on children on its website without the proper parental permission.⁴⁶



Brain power

By 2020, wind could provide one-tenth of our planet's electricity needs. Already today, SKF's innovative know-how is crucial to running a large proportion of the world's wind turbines.

Up to 25 % of the generating costs relate to maintenance. These can be reduced dramatically thanks to our systems for on-line condition monitoring and automatic lubrication. We help make it more economical to create cleaner, cheaper energy out of thin air.

By sharing our experience, expertise, and creativity, industries can boost performance beyond expectations. Therefore we need the best employees who can meet this challenge!

The Power of Knowledge Engineering

Plug into The Power of Knowledge Engineering.
Visit us at www.skf.com/knowledge

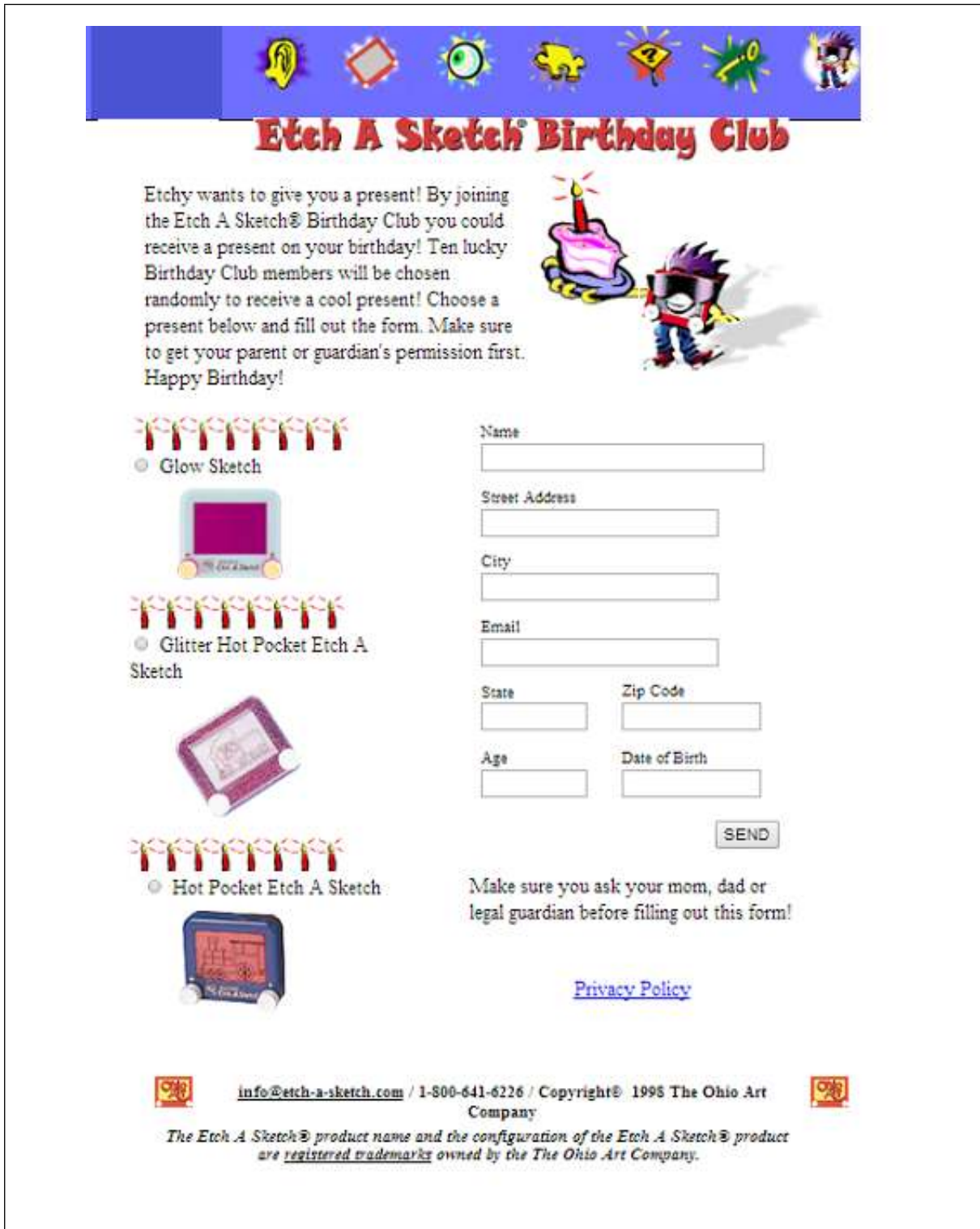
SKF

Download free eBooks at bookboon.com



Click on the ad to read more

(NOTE: COPPA is not the same law as COPA. COPA or the Children's Online Privacy Act is an anti-pornography declared unconstitutional and unenforceable by the U.S. District Court in 2007 and affirmed by the Third Circuit Court of Appeals in 2008.)



The form is titled "Etch A Sketch® Birthday Club" and features a decorative header with icons of a lightbulb, a diamond, a sun, a puzzle piece, a question mark, a key, and a character. The main text explains that members can win a present on their birthday. It lists three prize options: "Glow Sketch", "Glitter Hot Pocket Etch A Sketch", and "Hot Pocket Etch A Sketch". Each option is accompanied by a radio button and an image of the product. To the right of the text is an illustration of a character holding a birthday cake. Below the text is a registration form with fields for Name, Street Address, City, Email, State, Zip Code, Age, and Date of Birth. A "SEND" button is located below the form. At the bottom, there is a "Privacy Policy" link and a copyright notice for The Ohio Art Company.

Etchy wants to give you a present! By joining the Etch A Sketch® Birthday Club you could receive a present on your birthday! Ten lucky Birthday Club members will be chosen randomly to receive a cool present! Choose a present below and fill out the form. Make sure to get your parent or guardian's permission first. Happy Birthday!

Glow Sketch

Glitter Hot Pocket Etch A Sketch

Hot Pocket Etch A Sketch

Name

Street Address

City



Email

State Zip Code

Age Date of Birth

Make sure you ask your mom, dad or legal guardian before filling out this form!

[Privacy Policy](#)

 info@etch-a-sketch.com / 1-800-641-6226 / Copyright© 1998 The Ohio Art Company 

The Etch A Sketch® product name and the configuration of the Etch A Sketch® product are registered trademarks owned by the The Ohio Art Company.

Figure 2-9⁴⁷

2.7.4 Computer Fraud and Abuse Act of 1986⁴⁸

The Computer Fraud and Abuse Act (CFAA) is often referred to as “the federal anti-hacking law.” It sanctions criminal penalties for a person accessing a computer without authorization or exceeding their authorization. In 1994, the law was amended to provide also for civil penalties.⁴⁹

A key provision of the CFAA protects data stored in computers owned by or benefiting the U.S. government. The law also prohibits access to consumer information located in the records of a financial institution or of a consumer-reporting agency.

Activities Considered CFAA Violations
<ul style="list-style-type: none">• Obtaining national security information;• Compromising confidentiality;• Trespassing in a government computer;• Accessing to defraud and obtain value;• Damaging a computer or information;• Trafficking in passwords; or• Threatening to damage a computer.

Figure 2-10

The law is often criticized as being broadly written without clear definition of what constitutes crimes under the statute. It is an example of a law that has not been revised to reflect changes in technology.⁵⁰

The USA PATRIOT Act⁵¹ increased the scope and penalties of this law and first time offenders are now subject to imprisonment of 10 years.⁵²

2.7.5 Currency and Foreign Transactions Reporting Act of 1970⁵³

The Currency and Foreign Transactions Reporting Act of 1970 (also known as the “Bank Secrecy Act” or “BSA”), is a key money laundering statute in the United States. This law makes a federal crime to take the proceeds of an illegal activity and legitimize those funds, or to use secret bank accounts for criminal purposes. One of the most well known requirements of the law is the compulsion of businesses and financial institutions to report to the U.S. Treasury any cash transaction over \$10,000, or any suspicious financial activity.⁵⁴ This information provides law enforcement with evidence to investigate and prosecute currency violations. Under the BSA, companies and banks receiving these large funds are also required to maintain strict business records.⁵⁵

2.7.6 Electronic Communications Privacy Act of 1986⁵⁶

The Electronic Communications Privacy Act of 1986 (ECPA) is a combination of several laws. It includes the federal Wiretap Act⁵⁷ (Title I of the ECPA), the Stored Communications Act⁵⁸ (Title II of the ECPA), and the Pen-Register Act⁵⁹ (Title III of the ECPA).

According to the U.S. Department of Justice, the ECPA “protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.”⁶⁰

Exceptions to those required to comply with the ECPA include:

- Internet service providers (ISPs) other operators needing to access protected information in the “ordinary course of business”;
- Prior consent;
- Law enforcement or government officials authorized by law; or
- A probable cause search warrant issued by a federal court.

2.7.7 Fair Credit Reporting Act of 1970⁶¹

The Fair Credit Reporting Act of 1970 (FCRA) ensures consumer access to credit reports and scores. Additionally, consumers must be notified if they are denied credit because of negative information in their credit report. If incomplete or inaccurate information is included in a credit report (such as caused by identity theft), an individual may dispute that information, and the credit-reporting agency must correct or delete that incomplete information or data that cannot be verified. Consumers can also restrict the sharing of their credit reports to their employers.⁶²



“I studied English for 16 years but...
...I finally learned to speak it in just six lessons”
Jane, Chinese architect

ENGLISH OUT THERE

Click to hear me talking before and after my unique course download

The law was amended in 2003 by the Fair and Accurate Credit Transaction Act (FACTA),⁶³ and also requires the national credit reporting companies upon request, to provide a consumer with a free copy of their credit report every 12 months.

2.7.8 Family Educational Rights and Privacy Act⁶⁴

Congress passed FERPA (known as the Family Educational Rights and Privacy Act) in 1974 to protect the privacy and accuracy of student educational records. Under this law, student educational records are confidential and may not be released without written consent. If a student is under the age of 18 and enrolled in a public school district, the student's parents or legal guardian may enforce the student's privacy rights under FERPA. Once a student turns 18, or is under 18 and enrolled in a higher education institution, all FERPA rights belong to the student.⁶⁵

The law applies to all educational agencies and institutions who receive funding under any program administered by the U.S. Department of Education. This would include public K-12 school districts, community colleges, and four-year institutions. Private institutions rarely receive federal funds, and would not be required to follow FERPA guidelines.⁶⁶

The law grants a parent or student the right to:

1. Review the information that the institution is or have maintained about the student;
2. Seek to amend those records and if appropriate, append a statement to the record;
3. Consent to disclosure of his/her records; and
4. File a complaint with the Family Policy Compliance Office of the U.S. Department of Education.⁶⁷

Any records maintained by an institution directly related to a student are an educational record under FERPA.⁶⁸ However, some information, such as directory information, is deemed public and can be released without permission. This is information not regarded harmful or an invasion of privacy if disclosed, and it is often available in online student directories. However, the controlling person has the optional to keep directory information private upon notification to the educational institution.

Exclusions Under FERPA⁶⁹
<p>Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):</p> <ul style="list-style-type: none">○ School officials with legitimate educational interest;○ Other schools to which a student is transferring;○ Specified officials for audit or evaluation purposes;○ Appropriate parties in connection with financial aid to a student;○ Organizations conducting certain studies for or on behalf of the school;○ Accrediting organizations;○ To comply with a judicial order or lawfully issued subpoena;○ Appropriate officials in cases of health and safety emergencies; and○ State and local authorities, within a juvenile justice system, pursuant to specific State law.

Figure 2-11

2.7.9 Freedom of Information Act, 1966⁷⁰

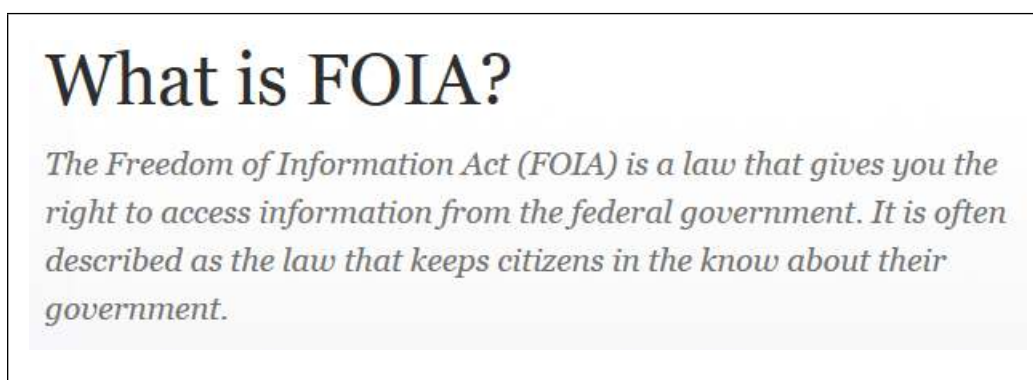


Figure 2-12⁷¹

The Freedom of Information Act (FOIA) is a 1966 federal law that gives individuals the right to access public information, and in particular federal agency records. Not all records can be requested under FOIA. The law restricts the release of records referred to as exclusions and exemptions. Congress has provided special protection in the FOIA for three narrow categories of law enforcement and national security records. The provisions protecting those records are known as “*exclusions*.” Records falling within an exclusion are not subject to the requirements of the FOIA.⁷² “Certain categories of information are not required to be released in response to a FOIA request because release would be harmful to governmental or private interests.” These categories of information are known as “*exemptions*.”⁷³ (See Figure 2-13)

Federal Records Exempt Under FOIA ⁷⁴
<ul style="list-style-type: none">• Records kept secret in the interest of national security and classified secret by a Presidential Executive Order;• Records that relate to the internal personnel rules and practices of a federal agency;• Records exempted by federal law;• Information containing trade secrets and commercial or financial information that is privileged or confidential;• Agency documents that would only be available through litigation;• Personnel and medical files that would be a personal privacy violation; and• Records or information compiled for law enforcement purposes.

Figure 2-13

2.7.10 Gramm-Leach-Bliley Act of 1999⁷⁵

This federal law instituted financial services privacy reform in the United States. It protects the privacy of consumers by requiring financial institutions to provide customers with written notice of the company’s privacy policies and practices. The Gramm-Leach-Bliley Act (GLBA) also limits the disclosure of nonpublic personal information about customers to third parties and allows consumers the ability to “opt out” of third party disclosure.⁷⁶

What do you want to do?

No matter what you want out of your future career, an employer with a broad range of operations in a load of countries will always be the ticket. Working within the Volvo Group means more than 100,000 friends and colleagues in more than 185 countries all over the world. We offer graduates great career opportunities – check out the Career section at our web site www.volvogroup.com. We look forward to getting to know you!

VOLVO
AB Volvo (publ)
www.volvogroup.com

VOLVO TRUCKS | RENAULT TRUCKS | MACK TRUCKS | VOLVO BUSES | VOLVO CONSTRUCTION EQUIPMENT | VOLVO PENTA | VOLVO AERO | VOLVO IT
VOLVO FINANCIAL SERVICES | VOLVO 3P | VOLVO POWERTRAIN | VOLVO PARTS | VOLVO TECHNOLOGY | VOLVO LOGISTICS | BUSINESS AREA ASIA



The law defines a consumer as an individual who obtains a financial product or service from a financial institution used primarily for personal, family, or household purposes.⁷⁷ It describes a financial institution as an organization “significantly engaged in financial activities,” including lending, exchanging, transferring, investing, or safeguarding money or securities.⁷⁸ It also includes issuing vendor credit cards, such as MasterCard, American Express, and Visa. Banks, credit unions, insurance companies, and savings and loans also qualify as a financial institution.⁷⁹

2.7.11 Health Insurance Portability and Accountability Act of 1996⁸⁰

The Health Insurance Portability and Accountability Act (HIPAA) provides privacy protection for “individually identifiable” information contained in health care related records collected and used by medical care providers.⁸¹ HIPAA requires health care suppliers (such a doctors, hospitals, and pharmacies) who collect medical information about patients to provide the consumer with a “Notice of Privacy Practices” that describes the personal information being collected and how the information is used.⁸² Under HIPAA, patients are required to sign a form stating they have received a copy of their privacy practices when they seek medical treatment.⁸³ The U.S. Office for Civil Rights enforces HIPAA privacy rules.

2.7.12 Privacy Act of 1974⁸⁴

The Privacy Act of 1974 established guidelines for federal agency disclosure of records and documents that contain personal information.⁸⁵ Personal information, such as name, photo, fingerprints, *etc.* cannot be released by the federal agency without the consent of the individual. The law, however, applies only to a “system of records.”⁸⁶ The law defines a system of records as “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”⁸⁷ Exceptions to release include a court order, a valid search warrant, or health and safety exceptions.⁸⁸

Each federal agency is required to publish in the *Federal Register*⁸⁹ the type of records under its control, their physical location, and the procedures for the release of such records.⁹⁰

Under the law, individuals also have the right to request changes to “records that are not accurate, relevant, timely, or complete.”⁹¹

2.7.13 Privacy Protection Act of 1980⁹²

This law prohibits law enforcement officers from illegally searching and seizing information from people who disseminate information to the public. The law is primarily intended to protect journalists and news reporters. This Act further requires police seek a search warrant to seize any work product created by journalists and news reporters “reasonably believed to have a purpose of dissemination to the public.”⁹³ Dissemination could be in a newspaper, book, television broadcast, an Internet video, or other similar form of public communication.⁹⁴

2.7.14 Right to Financial Privacy Act of 1978⁹⁵

Under the Right to Financial Privacy Act of 1978, the federal government is required to obtain a search warrant to access bank and financial records of individuals and companies (except in situations falling under the USA Patriot Act⁹⁶). The Patriot Act exception allows the disclosure of financial information to any intelligence or counterintelligence agency actively investigating international terrorism.⁹⁷

This law was a reaction to the case of *United States v. Miller*, 425 U.S. 435 (1976),⁹⁸ in which the Court held that customers did not have a right to privacy for their financial records.

2.7.15 Telephone Consumer Protection Act of 1991⁹⁹

The Telephone Consumer Protection Act of 1991, or TOPN, directs the Federal Communications Commission (FCC)¹⁰⁰ to establish regulations concerning telemarketing activities related to telephone solicitations and automatic dialers.¹⁰¹ The FCC rules require anyone making a telephone solicitation call to provide his or her name, the name of the person or entity on whose behalf the call made, and a telephone number or address at which that person or entity can be contacted.¹⁰²

TOPN provides that solicitors cannot use automatic dial telephone solicitations *if the called person is charged*, or send unsolicited advertisements to fax numbers. Additionally, vendors cannot make unsolicited telemarketing calls to police, fire, or other emergency numbers.¹⁰³

2.7.16 Video Privacy Protection Act of 1988¹⁰⁴

The Video Privacy Protection Act (VPPA) expanded the Cable Communications Privacy Act to restrict the disclosure of personally identifiable information for video rentals. The VPAA could also apply to the rental of games or movies over the Internet.¹⁰⁵

The VPPA was passed after the video rentals of a U.S. Supreme Court Justice Nominee, Robert Bork were disclosed to the public.¹⁰⁶

2.7.17 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept

and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT)¹⁰⁷

The USA Patriot Act was enacted in response to the terrorist attacks on the United States that took place on September 11, 2001. The law was passed to deter and punish terrorist acts in the United States and abroad.¹⁰⁸ According to the U.S. Department of Treasury, the goals of the law are:

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;
- To require all appropriate elements of the financial services industry to report potential money laundering;
- To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.¹⁰⁹

Critics of the law argue that the law is too broad and authorizes unnecessary surveillance of U.S. citizens. In 2011, Congress passed a four-year extension of three expiring Patriot Act provisions, keeping intact the all surveillance provisions.¹¹⁰

gaiTEYE[®]
Challenge the way we run

**EXPERIENCE THE POWER OF
FULL ENGAGEMENT...**

**RUN FASTER.
RUN LONGER..
RUN EASIER...**

**READ MORE & PRE-ORDER TODAY
WWW.GAITEYE.COM**

2.8 Administrative Agency Rules and Regulations

Several federal agencies are involved in investigating violations of federal privacy laws. These include the Federal Trade Commission, the U.S. Department of Education, the U.S. Department of Justice, and the U.S. Department of Treasury. These agencies publish rules and regulations related to the enforcement of privacy laws that found in the *Code of Federal Regulations* (CFR).¹¹¹

2.9 Summary

Privacy law in the United States is developed from five different sources: 1) the U.S. Constitution and Amendments, 2) state constitutions, 3) common law torts, 4) federal and state statutes, and 5) administrative agency rules and actions.

There is no express constitutional right to privacy, but the U.S. Supreme Court has held that privacy is a derived right. In addition, The Fourth, Fifth, Ninth, and Fourteenth Amendments are sources for this implicit right.

Invasion of privacy is a common law tort. This invasion can consist of intrusion, public disclosure of private facts, appropriation of name or likeness, or false light in the public eye.

Intrusion means intruding on a person's privacy, solitude, or seclusion. The intrusion can be physical by entering onto someone's property or by electronic or mechanical means. The tort does not require publications and the intrusion be offensive to a reasonable person.

Public disclosure of private facts involves the publications of private and embarrassing facts unrelated to matters of public concern. The disclosure of the private facts must be widespread. Therefore, information placed on the web can easily meet the disclosure requirement.

Appropriation of name or likeness occurs when someone's name, likeness, or identity is used for advertising or trade without the person's consent.

False light in the public eye exists when someone makes a false or misleading, highly offensive statement and creates a false impression to the public.

Remember that, for compliance, privacy law torts are based on common law and the precise requirements will vary from state to state.

Federal privacy laws were also reviewed in this chapter. These laws cover a variety of types of information including health, financial, and educational records.

2.10 Key Terms

Cable Communications Policy Act of 1984	Family Educations Rights and Privacy Act	Ninth Amendment
CAN-SPAM Act of 2003	Fifth Amendment	Privacy Act of 1974
Children’s Online Privacy Protection Act of 1998	Fourth Amendment	Privacy Protection Act of 1980
Computer Fraud and Abuse Act of 1986	Freedom of Information Act	Public disclosure of private facts
Currency and Foreign Transactions Act of 1970	Gramm-Leach-Bliley Act of 1999	Publically placing a person in a false light
Derived right	Health Insurance Portability and Accountability Act of 1996	Right to Financial Privacy Act of 1978
Electronic Communications Privacy Act of 1986	Implied right	Telephone Consumer Protection Act of 1991
Fair Credit Reporting Act of 1970	Intrusion upon seclusion	Video Privacy Protection Act of 1988
	Misappropriation of a person’s name or likeness	USA Patriot Act

2.11 Chapter Discussion Questions

1. What are the two major threats to privacy?
2. What are the five main sources of privacy law?
3. What is the difference between an express right and a derived right?
4. What is the significance of the case *Griswold v Connecticut* (1965) to privacy law?
5. What are the four main common law torts that address privacy law?
6. What is the difference between public disclosure of private facts and publically placing another in a false light?
7. Describe the CAN-SPAM Act of 1984.
8. Describe the Computer Fraud and Abuse Act of 1986.
9. How is FERPA important to a college student?
10. What is the difference between the Privacy Act of 1984 and the Privacy Protection Act of 1980?

2.12 Additional Learning Opportunities

The Electronic Privacy Information Center <<http://www.epic.org>>, describes itself as “is an independent non-profit research center in Washington, DC. EPIC works to protect privacy, freedom of expression, democratic values, and to promote the Public Voice in decisions concerning the future of the Internet.”¹¹² Its website includes information on emerging privacy issues.

2.13 Test Your Learning

1. Which of the following is not a source of privacy law?
 - A. The U.S. Constitution
 - B. The English Constitution
 - C. State constitutions
 - D. Federal statutes
 - E. State statutes

2. This Amendment to the U.S. Constitution is a safeguard against unreasonable searches and seizures:
 - A. 2nd
 - B. 4th
 - C. 5th
 - D. 9th
 - E. 14th



3. What is a tort?
 - A. A criminal case brought by the U.S. government against another private party for a wrong of one person against another.
 - B. A criminal case brought by a state government against another private party for a wrong of one person against another.
 - C. A civil case brought by the U.S. government against another private party for a wrong of one person against another.
 - D. A civil case brought by a state government against another private party for a wrong of one person against another.
 - E. A civil case brought by a private party against another private party for a wrong of one person against another.

4. Betsy accesses Kurt's bank account online without his permission. She simply views the information, and she does not attempt to access any funds from the account. Betsy's actions could constitute which of the following torts?
 - A. intrusion
 - B. misappropriation causing injury to a person's reputation
 - C. negligent use of a computer
 - D. public disclosure of public facts
 - E. publically placing a person in a false light

5. Will a U.S. Court issue a warrant to search person's Facebook® account without his or her knowledge?
 - A. No. The information is private and Facebook cannot be required to provide the information.
 - B. Maybe. The information is private and Facebook and can only be retrieved with a court order from the U.S. Attorney General.
 - C. Yes. The information is private; however, Facebook must give the information to law enforcement officials if Facebook has been served with a court order,
 - D. The information is always public and no warrant is ever needed.

6. Allie Kat keeps getting unsolicited text messages on her iPhone® from the *Astro Modeling News*. She has never done business with the company. This is a potential violation of what law?
 - A. Electronic Communications Privacy Act of 1986
 - B. Privacy Act of 1974
 - C. Privacy Protection Act of 1980
 - D. Right to Financial Privacy Act of 1978
 - E. Telephone Consumer Protection Act of 1991

7. C.B. is 6 ½ years old. He is very intelligent for his age and some might place his IQ at genius level. He decides to create a LinkedIn® account, but the application does not contain a certification clause that the user is over 13. LinkedIn is
 - A. violating COPPA because it failed to include a provision notifying parents of its privacy practices.
 - B. violating COPPA because it does not allow parents the ability to verify the personal information from its website.
 - C. violating COPPA because it does not have procedures in place to protect the confidentiality of the personal information collected.
 - D. not violating COPPA because LinkedIn is not a website directed to children under 13.

8. In reviewing the privacy policy for MEK Investments, Bobby finds a provision that states, “your data will be absolutely safe.” This statement
 - A. sets the company up for a lawsuit, as it is next to impossible to make that guarantee.
 - B. is a perfectly acceptable provision to include in a privacy policy.
 - C. violates the Online Personal Privacy Act.
 - D. fails to comply with federal law, as it does not state what type of personally identifiable information is being collected.

9. Which of the following is an incorrect statement?
 - A. Each state many have its own privacy laws.
 - B. Foreign laws may apply in certain circumstances in the U.S.
 - C. The greatest threat to privacy may come actually come from an individual person himself or herself.
 - D. None of these are correct.
 - E. All are correct.

10. The Privacy Protection Act (PPA) allows law enforcement agencies:
 - A. to seize books and newspapers that threaten First Amendment rights.
 - B. to seize materials from electronic publishers so long as Fourth Amendment requirements are met
 - C. both a and b
 - D. none of the above

Test Your Learning answers are located in the Appendix.