

Konnie G. Kustron



PRIVACY LAW

A U.S. Perspective

bookboon
The eBook company

KONNIE G. KUSTRON

**PRIVACY LAW:
A U.S. PERSPECTIVE**

Privacy Law: A U.S. Perspective

1st edition

© 2017 Konnie G. Kustron & bookboon.com

ISBN 978-87-403-1644-5

Peer review by Christopher Bezak

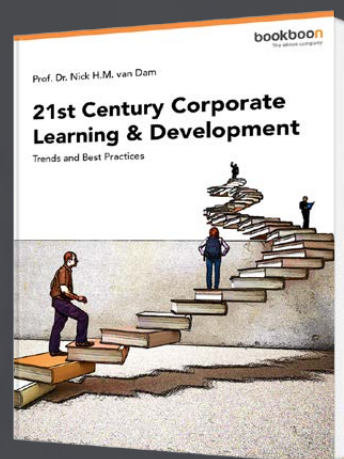
CONTENTS

	About the Author	8
1	What is Privacy?	9
1.1	Overview	9
1.2	Traditional Definitions	10
1.3	Historical Definitions	11
1.4	Is Privacy a Legal Right?	12
1.5	Sources of Privacy Law	14
1.6	U.S. Constitution	14
1.7	Case Law	19
1.8	Post <i>Griswold v. Connecticut</i>	25
1.9	Technology and Privacy	26
1.10	State Constitutions	31
1.11	Key Terms	32
1.12	Chapter Discussion Questions	32
1.13	Additional Learning Opportunities	33
1.14	Test Your Learning	34

Free eBook on Learning & Development

By the Chief Learning Officer of McKinsey

[Download Now](#)



2	Privacy Torts	36
2.1	Overview	36
2.2	Common Law Torts	37
2.3	Damages	38
2.4	Types of Privacy Torts	40
2.5	Public versus Private	40
2.6	Tort Category One: Intrusion	45
2.7	Defenses to Intrusion	46
2.8	Tort Category Two: Misappropriation	48
2.9	Defenses to Misappropriation	51
2.10	Category Three: Public Disclosure of Private Facts	52
2.11	Defenses to Public Disclosure of False Facts	53
2.12	Category Four: False Light	53
2.13	Defenses to False Light	55
2.14	Key Terms	55
2.15	Chapter Discussion Questions	55
2.16	Additional Learning Opportunities	55
2.17	Test Your Learning	56
3	Privacy at Home	59
3.1	Definition of a Home	59
3.2	<i>Mapp v. Ohio</i>	60
3.3	Curtilage	62
3.4	Sample Scenarios	64
3.5	The Sky	69
3.6	Privacy and Children	70
3.7	Privacy and the Internet of Things (IoT)	72
3.8	Data Breach Notification	74
3.9	Key Terms	76
3.10	Chapter Discussion Questions	76
3.11	Additional Learning Opportunities	76
3.12	Test Your Learning	77
4	Privacy Outside the Home	80
4.1	Overview	80
4.2	Education Privacy	81
4.3	Health Care Privacy	86
4.4	Financial Privacy	92
4.5	Voting Privacy	100
4.6	The Children's Internet Protection Act (CIPA)	101

4.7	Key Terms	101
4.8	Chapter Discussion Questions	102
4.9	Additional Learning Opportunities	103
4.10	Test Your Learning	103
5	Privacy at Work	106
5.1	Overview	106
5.2	The Pre-Employment Process	107
5.3	The Employee-Employer Relationship	111
5.4	Genetic Information Nondiscrimination Act (GINA)	118
5.5	Working at Home and BYOD (Bring Your Own Device)	120
5.6	Key Terms	121
5.7	Chapter Discussion Questions	121
5.8	Additional Learning Opportunities	121
5.9	Test Your Learning	122
6	Privacy and Government	125
6.1	Overview	125
6.2	The Privacy Act of 1974	127
6.3	U.S.A. Patriot Act	133
6.4	Traveler Surveillance and Screening	141
6.5	WikiLeaks	142
6.6	Edward J. Snowden	143
6.7	Public Information and the Freedom of Information Act	145
6.8	Key Terms	148
6.9	Chapter Discussion Questions	148
6.10	Additional Learning Opportunities	149
6.11	Test Your Learning	149
	Appendix: Test Your Learning Answers	152
	Endnotes	155



Dedicated to my Mother, Margaret who was an inspiration to her children
and grandchildren and always challenged them to do their best.
1927–2016

Note: Court cases, Illustrations, and photographs used in this book have been taken primarily from United States government websites. As such, they are public documents belonging to the United States government (17 U.S.C. § 105), and as such, are not subject to U.S. copyright protection. Included materials are available at various websites including <https://public.resouce.org>. Other documents have been included for educational purposes and discussion.

As used in this text: TWITTER, TWEET, RETWEET and the Twitter logo are trademarks of Twitter, Inc. or its affiliates; Facebook is a trademark under the group of companies and trademarks under the Facebook brand.

Images designated as “used with permission” are owned by the author.

Any errors or omissions are the sole responsibility of the author.

ABOUT THE AUTHOR

Konnie Kustron is an attorney-educator. She is currently a professor in in the School of Technology and Professional Services Management at Eastern Michigan University in Ypsilanti, Michigan.

Professor Kustron received her B.S. with honors in pre-law from Michigan State University, and her J.D. from the Michigan State University, College of Law. She is a member of the Michigan Bar and approved as a Veteran's Affairs attorney with United States Department of Veteran's Affairs. Professor Kustron is the recipient of an Eastern Michigan University Alumni Teaching Award as well as the Dean's Outstanding Faculty Award. Recently, she has been a contributor to the *Encyclopedia of Mathematics and Society* (Salem Press, 2011), which was described as the "Best Reference 2011," by the *Library Journal* – a leading reviewer of library materials in the United States. Professor Kustron is also a chapter author in the *Internet Guide for Michigan Lawyers*, a winner of the "Award of Excellence in the Best Publication" category awarded by the Association for Continuing Legal Education.

In 2013 Mrs. Kustron published her first Bookboon text, *Introduction to the American Legal System* available at <http://bookboon.com/en/introduction-to-the-american-legal-system-ebook>. Her second Bookboon text, *Internet Law: A U.S. Perspective* was published in 2015.

About the Contributing Reviewer

Christopher Bezak is an attorney specializing in intellectual property law at Sughrue Mion, PLLC, in Washington, D.C. Mr. Bezak received his B.S. with honors in Computer Engineering from the University of Michigan, Ann Arbor, and his J.D. with honors from the Michigan State University, College of Law. Mr. Bezak is licensed to practice law in the State of Michigan as well as before the U.S. Patent and Trademark Office.

1 WHAT IS PRIVACY?

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

- Define privacy from a personal perspective;
- Explain the historical evolution of the definition of privacy;
- Discuss the federal constitutional implications of privacy;
- Explain how and why legal authority is used by a court in its decision making process;
- Identify the federal Constitutional Amendments that have been applied to privacy rights; and
- Explain the significance of the U.S. Supreme Court ruling in *Griswold v. Connecticut* as it relates to personal privacy rights.

1.1 OVERVIEW

To begin a discussion of **privacy**, the best starting point for that conversation is to establish a working definition of the word. However, if you were to gather together a group of people in a room, you would quickly find that the concept of privacy has different meanings to each person, depending on his or her personal perspective.

For example, does privacy mean the **right to be left alone**? Does it mean the **right to keep personal information private**? Or, does it simply mean to **be free from surveillance by others**? Some, taking a more pragmatic view, may simply respond to the discussion with a lack of interest, taking the position that with today's technology, there is no such thing as personal privacy. In other words, "privacy is dead."¹

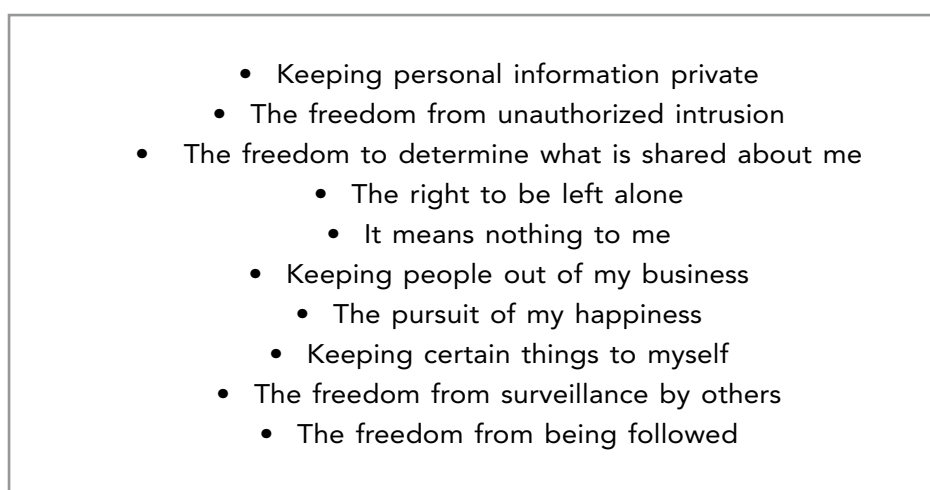
- 
- Keeping personal information private
 - The freedom from unauthorized intrusion
 - The freedom to determine what is shared about me
 - The right to be left alone
 - It means nothing to me
 - Keeping people out of my business
 - The pursuit of my happiness
 - Keeping certain things to myself
 - The freedom from surveillance by others
 - The freedom from being followed

Figure 1-1: What is your definition of privacy?

1.2 TRADITIONAL DEFINITIONS

As you have just read, there are many ways to define privacy. Some of the descriptions presented are simple, while others are more complex. So, let's begin our discussion of privacy using a common reference point by determining a working definition for this word.

For example, *The Oxford Dictionary* describes privacy as “(a) state in which one is not observed or disturbed by other people,” and “the state of being free from public attention.”² On the other hand, dictionary.com (based on the *Random House Dictionary*) defines privacy as 1) “the state of being apart from other people or concealed from their view; solitude; seclusion”; 2) “the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone”; and 3) “freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one's personal data or information, as by a government, corporation, or individual.”³

Some similarities are obvious when comparing the above definitions. First is the language “state of being free from” public attention or unwarranted intrusion. Second, both publishers suggest a right to be left alone. In other words, the definitions imply that privacy includes a physical and spatial element being away from others.⁴

The definitions presented by *The Oxford Dictionary* and the *Random House Dictionary* have a traditional focus that does not include technology. Now, in the 21st Century, with technology being so engrained in everyday living, some proposals modify these definitions from the physical aspect of privacy to include the element of *being able to control personal information*. The **International Association of Privacy Professionals** (IAPP), the largest privacy organization in the world, provides one such proposal. The IAPP states that privacy is “the right to be let alone, or freedom from interference or intrusion.” But, IAPP distinguishes privacy from “**information privacy**,” which is “the right to have some control over how your personal information is collected and used.”⁵ Both privacy and information privacy will be discussed in this book.

Safe Havens

Consistent with the right to be left alone, it is generally agreed that there are certain safe havens of privacy (called privacy zones) such as your home where a person can expect to be safe from intrusion by others including law enforcement officials. This privacy zone ceases to exist once a person walks out of his or her home. This means that drones can fly over your home at 100 feet and take photos of you in your backyard. This also means that cameras located at the top of traffic light posts can record the movement of you driving your car. In fact, any person can take a photo of you in any public place (note, a public restroom is considered private and a safe haven), and post that photo on the Internet with little or no legal consequence.



Figure 1-2: Used with permission⁶

1.3 HISTORICAL DEFINITIONS

Legal scholars state that the first use of the term privacy can be attributed to the 1890 *Harvard Law Review* article “Right to Privacy”⁷ written by Samuel Warren and the future U.S. Supreme Court Justice Louis Brandeis. In their article, citing another future U.S. Supreme Court Justice Thomas Cooley,⁸ they describe privacy simply as “the right to be left alone.”⁹

The authors also acknowledged in their article how “new inventions” were challenging privacy rights. These new inventions included “cameras and photography,” as well as the growing presence and ease of printing newspapers in the United States. These papers often included “social news” describing births, weddings, and deaths of well-known members of the community. Little could Warren and Brandeis predict the challenges to privacy that technology would bring almost 125 years later.¹⁰

“Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual the right ‘to be let alone’... Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”⁶

– Louis Brandeis in the “Right to Privacy”

1.4 IS PRIVACY A LEGAL RIGHT?

When studying privacy, there are two questions that need to be asked. First, is privacy a **legal right**, as suggested by Warren and Brandeis? Second, if privacy is a legal right, then what is the basis for acknowledging this right?¹¹

1.4.1 COURT SYSTEMS

We begin the process of answering these questions by looking at the legal system and courts in the United States. In the U.S., there are two types of court systems: **federal** and **state**. Considering there are fifty states in the U.S., this means there are fifty-one court systems. However, there are similarities in how the court systems operate.

Each of these court systems will consist of a **trial court** and an **appellate court** at which parties can challenge a trial court's decision and request a review of the trial court's ruling. Table 1-1 below provides a comparison of the federal and state courts.



www.sylvania.com

We do not reinvent
the wheel we reinvent
light.

Fascinating lighting offers an infinite spectrum of possibilities: Innovative technologies and new markets provide both opportunities and challenges. An environment in which your expertise is in high demand. Enjoy the supportive working atmosphere within our global group and benefit from international career paths. Implement sustainable ideas in close cooperation with other specialists and contribute to influencing our future. Come and join us in reinventing light every day.

Light is OSRAM

OSRAM
SYLVANIA



The Federal Court System	The State Court System
<p>Article III of the Constitution invests the judicial power of the United States in the federal court system. Article III, Section 1 specifically creates the U.S. Supreme Court and gives Congress the authority to create the lower federal courts.</p>	<p>The Constitution and laws of each state establish the state courts. A court of last resort, often known as a Supreme Court, is usually the highest court. Some states also have an intermediate Court of Appeals. Below these Courts of Appeals are the state trial courts. Some are referred to as Circuit or District Courts.</p>
<p>Congress has used this power to establish the 13 U.S. Courts of Appeals, the 94 U.S. District Courts, the U.S. Court of Claims, and the U.S. Court of International Trade. U.S. Bankruptcy Courts handle bankruptcy cases. Magistrate Judges handle some District Court matters.</p>	<p>States also usually have courts that handle specific legal matters, e.g., probate court (wills and estates), juvenile court, family court, etc.</p>
<p>Parties dissatisfied with a decision of a U.S. District Court, the U.S. Court of Claims, and/or the U.S. Court of International Trade may appeal to a U.S. Court of Appeals.</p>	<p>Parties dissatisfied with the decision of the trial court (e.g., Circuit or District Courts) may appeal to the intermediate Court of Appeals.</p>
<p>A party may ask the U.S. Supreme Court to review a decision of the U.S. Court of Appeals, but the Supreme Court usually is under no obligation to do so. The U.S. Supreme Court is the final arbiter of federal constitutional questions.</p>	<p>Parties have the option to appeal to the highest state court.</p>
	<p>Only certain cases are eligible for review by the U.S. Supreme Court.</p>

Table 1-1: A comparison of the federal and state court systems – Materials in the public domain¹²

1.4.2 LEGAL AUTHORITY

Courts base their decisions on **legal authority**. Legal authority is the value a court places on certain legal documents and materials when making a decision. These materials may be divided into two categories: **primary authority** and **secondary authority**. Courts rely on primary authority as their first reference when adjudicating a dispute, and may resort to secondary authority as necessary to supplement primary authority.

Table 1-2 presents a *ranked* list of primary authority. The higher ranked materials on the list are more important and persuasive to a court in rendering its decision. For example, if an attorney is presenting a case in federal court arguing that the U.S. Constitution is the relevant and applicable authority in a case, and the opposing counsel argues that a federal statute is the applicable law, who has the stronger argument? Using Table 1-2, the attorney using the U.S. Constitution would have the stronger and more persuasive argument than the lawyer arguing the applicability of a federal law (statute).¹³

1. United States Constitution
2. Treaties
3. Acts of Congress (Federal Statutes)
4. U.S. Court Cases (U.S. Supreme Court, U.S. Courts of Appeals, U.S. Districts Courts)
5. Federal Court Rules (Civil and Criminal) and Federal Evidentiary Rules
6. U.S. Administrative Agency Rules, Regulations and Orders
7. U.S. Attorney General Opinions
8. State Constitutions
9. State Court Cases (Supreme Court, Appellate Court, Trial Court)
10. State Court Rules (Civil and Criminal) and State Evidentiary Rules
11. State Administrative Agency Rules, Regulations and Orders
12. Municipal Ordinances
13. State Attorney General Opinions

Table 1-2: Hierarchy of "Primary" Authority

Secondary authority includes other types of materials supplemental to primary authority, such as scholarly legal journals, legal dictionaries, and legal encyclopedias. Courts are not required to reference secondary authority when promulgating a court ruling.

1.5 SOURCES OF PRIVACY LAW

U.S. privacy law is based on five legal sources: 1) the **U.S. Constitution and Amendments**, 2) **state constitutions**, 3) **common law torts** (discussed primarily in state court opinions), 4) **federal and state statutes**, and 5) **administrative agency rules and actions**. The following will discuss how the first source, the U.S. Constitution and the Amendments relate to privacy rights. Note that these five sources are considered primary authority.

1.6 U.S. CONSTITUTION

Most Americans believe the U.S. Constitution protects personal privacy rights.¹⁴ However, if you review the Constitution and its Amendments, there is not one specific mention of the word privacy. In other words, perhaps to the surprise of many, there is no express right to privacy written in the U.S. Constitution.

Instead, privacy rights in the Constitution are **derived or implied rights**. This means that the Courts, in reviewing the Constitution, have found these rights implicitly exist in the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.

1.6.1 FIRST AMENDMENT

The **First Amendment** explicitly protects **five freedoms**: speech, religion, press, petition, and assembly. It states: “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.” Privacy advocates argue that the First Amendment protects privacy because each of the five freedoms presents an element of personal choice, protected by the Constitution.



Discover the truth at www.deloitte.ca/careers

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

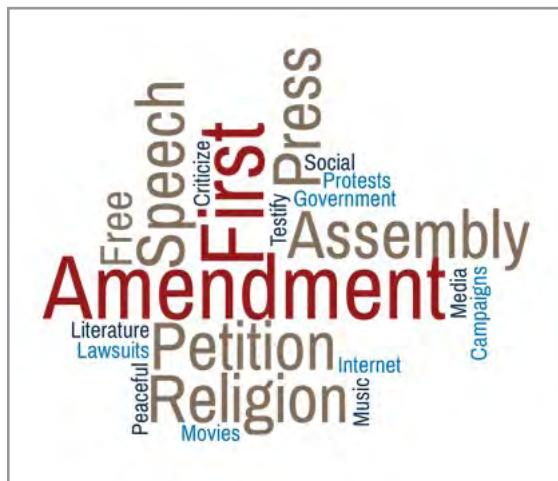


Figure 1-3: First Amendment Word Cloud – Materials in the public domain¹⁵

1.6.2 THIRD AMENDMENT

The **Third Amendment** protects individuals from being forced to house militia in their home.¹⁶ This means that a person’s home is respected as being within a “zone of privacy.”

1.6.3 FOURTH AMENDMENT

The **Fourth Amendment** protects an individual’s right against unreasonable searches and seizure. It places a balance between legitimate government interests and intrusion¹⁷ by the government from a person and their possessions.

What Does the Fourth Amendment Mean?

The Constitution, through the Fourth Amendment, protects people from unreasonable searches and seizures by the government. The Fourth Amendment, however, is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law.

Figure 1-4: U.S. Courts interpretation of the Fourth Amendment – Materials in the public domain¹⁸

1.6.4 FIFTH AMENDMENT

The **Fifth Amendment** protects a person against **self-incrimination**. Self-incrimination means testifying against oneself in a legal proceeding. This Amendment is more commonly associated with what is known as a **Miranda warning**, which law enforcement officials are required to administer to a person upon arrest. The components of a Miranda warning are detailed in the table below.





Figure 1-5: Required steps in the Miranda Process – Materials in the public domain¹⁹

SIMPLY CLEVER

ŠKODA



We will turn your CV into an opportunity of a lifetime



Do you like cars? Would you like to be a part of a successful brand? We will appreciate and reward both your enthusiasm and talent. Send us your CV. You will be surprised where it can take you.

Send us your CV on www.employerforlife.com



1.6.5 NINTH AMENDMENT

The **Ninth Amendment** states “[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.” This means “that the list of rights enumerated in the Constitution is not exhaustive, and that the people retain all rights not enumerated.”²⁰ This means a person may have additional rights, such as privacy rights, that are not specifically provided in the first eight Amendments of the U.S. Constitution.²¹

1.6.6 FOURTEENTH AMENDMENT

The **Fourteenth Amendment** expands federal protection to the states, and affords individuals with due process and equal protection to the states.²² It states in that “(a)ll persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.”²³

1.7 CASE LAW

Many cases have discussed privacy rights and the relationship of privacy to the U.S. Constitution. One early decision is *Meyer v. Nebraska*,²⁴ 262 U.S. 390 (1923),²⁵ in which the Court broadly defined the word “liberty” in the Fourteenth Amendment to include the right of privacy with respect to parental choices of the education for their children. At issue in this case was the validity of a Nebraska state law prohibiting the teaching of the German language to students until reaching the ninth grade. The law was successfully challenged by parents of German heritage, who wanted their children to learn the German language at a younger age.

A quote from *Meyer v. Nebraska*, 262, U.S. 390, 399 (1923)

“While this Court has not attempted to define with exactness the liberty thus guaranteed, the term has received much consideration and some of the included things have been definitely stated. Without doubt, it denotes not merely freedom from bodily restraint, but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men...”

In 1925, the U.S. Supreme Court looked at privacy rights again from another educational perspective in the case of *Pierce v. Society of Sisters*.²⁶ In *Pierce*, relying on *Meyer*, the Court invalidated a state law requiring students to attend only public schools, and ruled that children may attend any type of private or parochial school.

Approximately 40 years later and relying on the Bill of Rights, Justice William Douglas agreed with Warren and Brandeis and their privacy definition (*i.e.*, “the right to be left alone”) in the landmark birth control case of *Griswold v. Connecticut*, 381 U.S. 479.²⁷ In *Griswold*, the “Executive Director of the Planned Parenthood League of Connecticut, and its medical director, a licensed physician, were convicted as accessories for giving married persons (*sic*) information and medical advice on how to prevent conception and, following examination, prescribing a contraceptive device or material for the wife’s use.”²⁸ This conviction was based on a violation of Connecticut state law. However, the U.S. Supreme Court disagreed with the lower court, and reversed its ruling, holding that “(t)he Connecticut statute forbidding use of contraceptives violates the right of marital privacy which is within the penumbra of specific guarantees of the Bill of Rights.”²⁹

So, what is a *penumbra of guarantees* in the Bill of Rights? To answer that question, see text from key sections of the *Griswold* case below. Keep in mind as you read *Griswold*, the Constitutional Amendments protect individuals against federal *government* invasion of privacy only – not invasion of privacy by other individuals.

***Griswold v Connecticut*, 381 U.S. 479 (1965)**³⁰

Opinion by Justice Douglas

Appellant Griswold is Executive Director of the Planned Parenthood League of Connecticut. Appellant Buxton is a licensed physician and a professor at the Yale Medical School who served as Medical Director for the League at its Center in New Haven – a center open and operating from November 1 to November 10, 1961, when appellants were arrested.

They gave information, instruction, and medical advice to *married persons* as to the means of preventing conception. They examined the wife and prescribed the best contraceptive device or material for her use. Fees were usually charged, although some couples were serviced free.

The statutes whose constitutionality is involved in this appeal are §§ 53–32 and 54–196 of the General Statutes of Connecticut (1958 rev.). The former provides: Any person who uses any drug, medicinal article or instrument for the purpose of preventing conception shall be fined not less than fifty dollars or imprisoned not less than sixty days nor more than one year or be both fined and imprisoned.

Section 54–196 provides:

Any person who assists, abets, counsels, causes, hires or commands another to commit any offense may be prosecuted and punished as if he were the principal offender.

The appellants were found guilty as accessories and fined \$100 each, against the claim that the accessory statute, as so applied, violated the Fourteenth Amendment...

The association of people is not mentioned in the Constitution nor in the Bill of Rights. The right to educate a child in a school of the parents’ choice – whether public or private or parochial – is also not mentioned. Nor is the right to study any particular subject or any foreign language. Yet the First Amendment has been construed to include certain of those rights.




- The number 1 MOOC for Primary Education
- Free Digital Learning for Children 5-12
- 15 Million Children Reached

About e-Learning for Kids Established in 2004, e-Learning for Kids is a global nonprofit foundation dedicated to fun and free learning on the Internet for children ages 5 - 12 with courses in math, science, language arts, computers, health and environmental skills. Since 2005, more than 15 million children in over 190 countries have benefitted from eLessons provided by EFKI. An all-volunteer staff consists of education and e-learning experts and business professionals from around the world committed to making difference. eLearning for Kids is actively seeking funding, volunteers, sponsors and courseware developers; get involved! For more information, please visit www.e-learningforkids.org.

By *Pierce v. Society of Sisters*, *supra*, the right to educate one's children as one chooses is made applicable to the States by the force of the First and Fourteenth Amendments. By *Meyer v. Nebraska*, *supra*, the same dignity is given the right to study the German language in a private school. In other words, the State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge. The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read (*Martin v. Struthers*, 319 U.S. 141, 143) and freedom of inquiry, freedom of thought, and freedom to teach (*see Wiemann v. Updegraff*, 344 U.S. 183, 195) – indeed, the freedom of the entire university community. *Sweezy v. New Hampshire*, 354 U.S. 234, 249–250, 261–263; *Barenblatt v. United States*, 360 U.S. 109, 112; *Baggett v. Bullitt*, 377 U.S. 360, 369. Without [p. 483] those peripheral rights, the specific rights would be less secure. And so we reaffirm the principle of the *Pierce* and the *Meyer* cases.

In *NAACP v. Alabama*, 357 U.S. 449, 462 we protected the “freedom to associate and privacy in one's associations,” noting that freedom of association was a peripheral First Amendment right. Disclosure of membership lists of a constitutionally valid association, we held, was invalid as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association. *Ibid.* In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion. In like context, we have protected forms of “association” that are not political in the customary sense, but pertain to the social, legal, and economic benefit of the members. *NAACP v. Button*, 371 U.S. 415, 430–431. In *Schwartz v. Board of Bar Examiners*, 353 U.S. 232, we held it not permissible to bar a lawyer from practice because he had once been a member of the Communist Party. The man's “association with that Party” was not shown to be “anything more than a political faith in a political party” (*id.* at 244), and was not action of a kind proving bad moral character. *Id.* at 245–246.

Those cases involved more than the “right of assembly” – a right that extends to all, irrespective of their race or ideology. *De Jonge v. Oregon*, 299 U.S. 353. The right of “association,” like the right of belief (*Board of Education v. Barnette*, 319 U.S. 624), is more than the right to attend a meeting; it includes the right to express one's attitudes or philosophies by membership in a group or by affiliation with it or by other lawful means. Association in that context is a form of expression of opinion, and, while it is not expressly included in the First Amendment, its existence is necessary in making the express guarantees fully meaningful. [p. 484]

The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. See *Poe v. Ullman*, 367 U.S. 497, 516–522 (dissenting opinion). Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers “in any house” in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.”

The Fourth and Fifth Amendments were described in *Boyd v. United States*, 116 U.S. 616, 630, as protection against all governmental invasions “of the sanctity of a man’s home and the privacies of life.” We recently referred [p. 485] in *Mapp v. Ohio*, 367 U.S. 643, 656, to the Fourth Amendment as creating a “right to privacy, no less important than any other right carefully and particularly reserved to the people.” ... We have had many controversies over these penumbral rights of “privacy and repose.” ... These cases bear witness that the right of privacy which presses for recognition here is a legitimate one.

The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees. And it concerns a law which, in forbidding the use of contraceptives, rather than regulating their manufacture or sale, seeks to achieve its goals by means having a maximum destructive impact upon that relationship. Such a law cannot stand in light of the familiar principle, so often applied by this Court, that a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.

NAACP v. Alabama, 377 U.S. 288, 307. Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The [p. 486] very idea is repulsive to the notions of privacy surrounding the marriage relationship.

We deal with a right of privacy older than the Bill of Rights – older than our political parties, older than our school system. Marriage is a coming together for better or for worse, hopefully enduring, and intimate to the degree of being sacred. It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects. Yet it is an association for as noble a purpose as any involved in our prior decisions.

Reversed.




Figure 1-6: Used with permission³¹

Cynthia | AXA Graduate

AXA Global Graduate Program

Find out more and apply

redefining / standards 

1.8 POST *GRISWOLD V. CONNECTICUT*

After *Griswold*, the Supreme Court continued to explore and expand privacy rights in its written decisions. While *Griswold* focused on marital privacy rights, the 1972 case *Eisenstadt v. Baird*, 405 U.S. 438 (1972)³² reviewed the legality of allowing unmarried individuals to purchase contraceptive devices. In *Eisenstadt*, Appellee “William Baird gave away Emko Vaginal Foam to a woman following his Boston University lecture on birth control and over-population. Massachusetts charged Baird with a felony, to distribute contraceptives to unmarried men or women. Under the law, only married couples could obtain contraceptives; only registered doctors or pharmacists could provide them. Baird was not an authorized distributor of contraceptives.”³³ The question in this case was whether the state statute was a violation of the right to privacy as outlined in *Griswold* and applicable to Massachusetts under the Fourteenth Amendment. The Court found that the statute was unconstitutional, but not on privacy grounds *per se*. However, Justice Brennan stated in the Court’s opinion: “If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.”³⁴

Similarly, in *Roe v. Wade*, 410 U.S. 113 (1973),³⁵ an unmarried woman Roe and a married couple (the Does) challenged a Texas law that prohibited the right to terminate a pregnancy, which limited abortion only to save the mother’s life. Plaintiffs argued “that (the State of Texas) abridged (their) right of personal privacy, protected by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments.”³⁶ In its opinion in favor of *Roe*, the Court reiterated that “(t)he Constitution does not explicitly mention any right of privacy,” but “the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution.”³⁷ This case ultimately legalized abortion in the United States.

Courts have also looked at privacy rights from a criminal perspective. For example, in *Katz v. United States*, 389 U.S. 347 (1967),³⁸ FBI agents acting without a search warrant attached an “electronic listening and recording device to the outside of a public phone booth to gather evidence of illegal bookmaking.”³⁹ The United States Supreme Court held the actions of the FBI violated the Fourth Amendment search warrant requirements because the defendant was entitled to a reasonable expectation of privacy when in a phone booth. Accordingly, because the Fourth Amendment protects unreasonable search and seizures, under both federal or state law there must be probable cause for an immediate search, or otherwise, the search must be accompanied by a warrant authorized by a court.⁴⁰

1.9 TECHNOLOGY AND PRIVACY

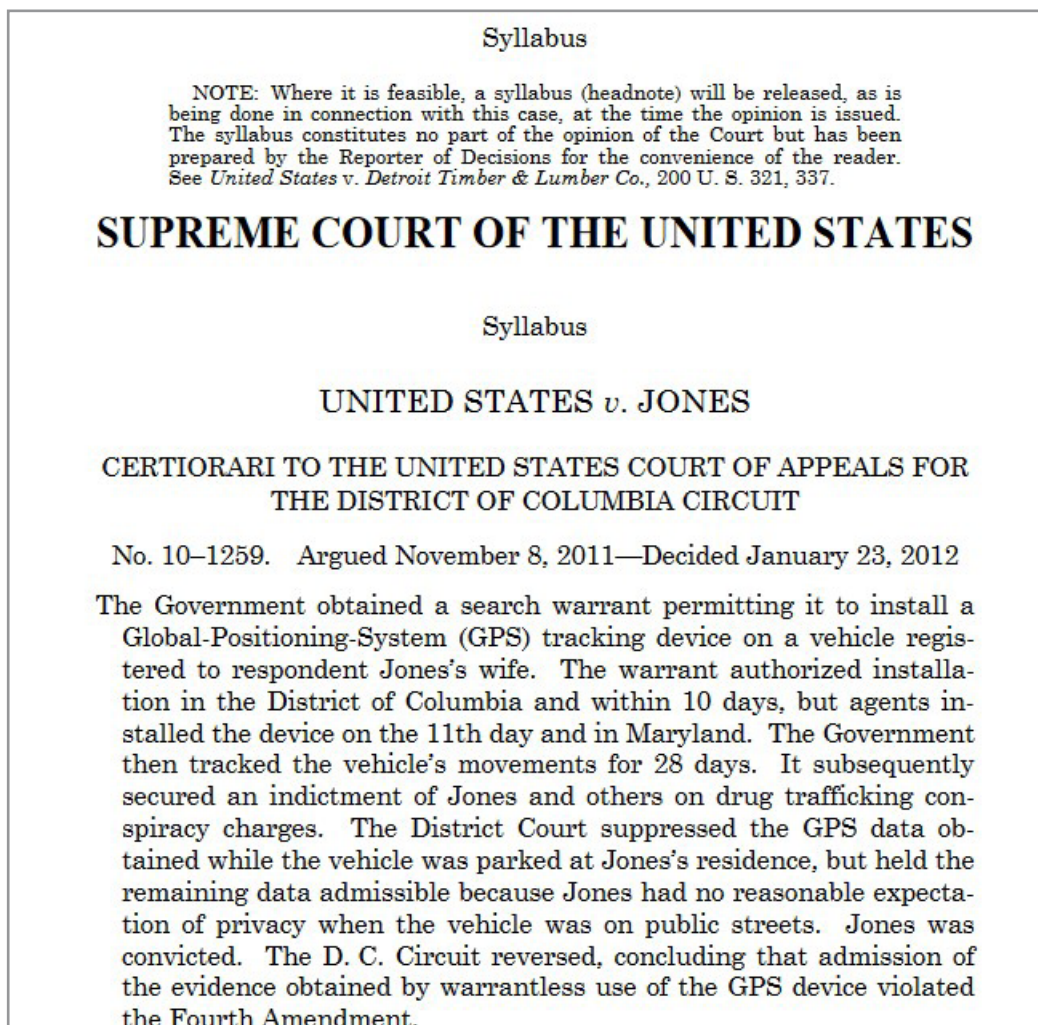


Figure 1-7: Materials in the public domain⁴¹

Laws written in the past have not always prepared to adapt for changes in technology. Thus, legislatures and courts continue to redefine privacy in a continuous “catch-up” mode. Cases such as *Maryland v. King*, 569 U.S. ___, 133 S.Ct. 1958 (2013)⁴² (in which the Court agreed that law enforcement officials have the right to take DNA samples of those incarcerated), *Kyllo v. United States*, 533 U.S. 27 (2001)⁴³ (in which the Court agreed “thermal-imaging device to detect relative amounts of heat emanating from a private home constitute an unconstitutional search in violation of the Fourth Amendment”⁴⁴), and *United States v. Jones*, 565 U.S. ___, 132 S.Ct. 945 (2012)⁴⁵ (in which the Court determined that a GPS device constituted a search and required a warrant and that law enforcement), continue to challenge the privacy rights implied from the U.S. Constitution. Indeed, because laws change at a much slower speed than technology, the issue of privacy and the courts will continue to exist for years to come. The *Quon* case below, is an example of how the challenges of privacy and technology collide.

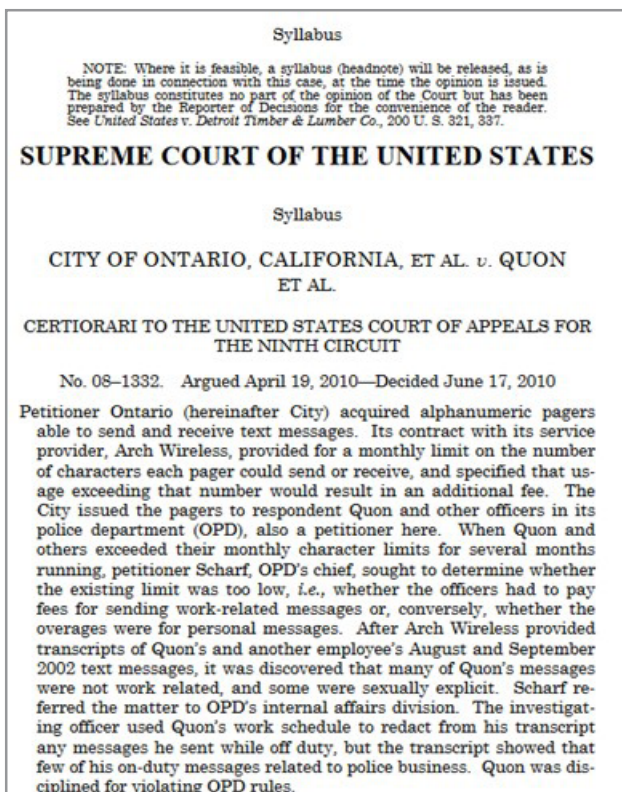


Figure 1-8: Materials in the public domain⁴⁶

I joined MITAS because
I wanted **real responsibility**

The Graduate Programme
for Engineers and Geoscientists
www.discovermitas.com

Month 16

I was a construction supervisor in the North Sea advising and helping foremen solve problems

Real work
International opportunities
Three work placements

City of Ontario, California v. Quon, 560 U.S. 746 (2010)⁴⁷

Opinion by Justice Kennedy

This case involves the assertion by a government employer of the right, in circumstances to be described, to read text messages sent and received on a pager the employer owned and issued to an employee. The employee contends that the privacy of the messages is protected by the ban on “unreasonable searches and seizures” found in the Fourth Amendment to the United States Constitution, made applicable to the States by the Due Process Clause of the Fourteenth Amendment. *Mapp v. Ohio*, 367 U.S. 643 (1961). Though the case touches on issues of far-reaching significance, the Court concludes it can be resolved by settled principles determining when a search is reasonable.

The City of Ontario (City) is a political subdivision of the State of California. The case arose out of incidents in 2001 and 2002 when respondent Jeff Quon was employed by the Ontario Police Department (OPD). He was a police sergeant and member of OPD’s Special Weapons and Tactics (SWAT) Team. The City, OPD, and OPD’s Chief, Lloyd Scharf, are petitioners here. As will be discussed, two respondents share the last name Quon. In this opinion “Quon” refers to Jeff Quon, for the relevant events mostly revolve around him.

In October 2001, the City acquired 20 alphanumeric pagers capable of sending and receiving text messages. Arch Wireless Operating Company provided wireless service for the pagers. Under the City’s service contract with Arch Wireless, each pager was allotted a limited number of characters sent or received each month. Usage in excess of that amount would result in an additional fee. The City issued pagers to Quon and other SWAT Team members in order to help the SWAT Team mobilize and respond to emergency situations.

Before acquiring the pagers, the City announced a “Computer Usage, Internet and E-Mail Policy” (Computer Policy) that applied to all employees. Among other provisions, it specified that the City “reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.” App. to Pet. for Cert. 152a. In March 2000, Quon signed a statement acknowledging that he had read and understood the Computer Policy.

The Computer Policy did not apply, on its face, to text messaging. Text messages share similarities with e-mails, but the two differ in an important way. In this case, for instance, an e-mail sent on a City computer was transmitted through the City’s own data servers, but a text message sent on one of the City’s pagers was transmitted using wireless radio frequencies from an individual pager to a receiving station owned by Arch Wireless. It was routed through Arch Wireless’ computer network, where it remained until the recipient’s pager or cellular telephone was ready to receive the message, at which point Arch Wireless transmitted the message from the transmitting station nearest to the recipient. After delivery, Arch Wireless retained a copy on its computer servers. The message did not pass through computers owned by the City.

Although the Computer Policy did not cover text messages by its explicit terms, the City made clear to employees, including Quon, that the City would treat text messages the same way as it treated e-mails. At an April 18, 2002, staff meeting at which Quon was present, Lieutenant Steven Duke, the OPD officer responsible for the City's contract with Arch Wireless, told officers that messages sent on the pagers "are considered e-mail messages. This means that [text] messages would fall under the City's policy as public information and [would be] eligible for auditing." App. 30. Duke's comments were put in writing in a memorandum sent on April 29, 2002, by Chief Scharf to Quon and other City personnel.

Within the first or second billing cycle after the pagers were distributed, Quon exceeded his monthly text message character allotment. Duke told Quon about the overage, and reminded him that messages sent on the pagers were "considered e-mail and could be audited." *Id.*, at 40. Duke said, however, that "it was not his intent to audit [an] employee's text messages to see if the overage [was] due to work related transmissions." *Ibid.* Duke suggested that Quon could reimburse the City for the overage fee rather than have Duke audit the messages. Quon wrote a check to the City for the overage. Duke offered the same arrangement to other employees who incurred overage fees.

Over the next few months, Quon exceeded his character limit three or four times. Each time he reimbursed the City. Quon and another officer again incurred overage fees for their pager usage in August 2002. At a meeting in October, Duke told Scharf that he had become "tired of being a bill collector." *Id.*, at 91. Scharf decided to determine whether the existing character limit was too low – that is, whether officers such as Quon were having to pay fees for sending work-related messages – or if the overages were for personal messages. Scharf told Duke to request transcripts of text messages sent in August and September by Quon and the other employee who had exceeded the character allowance.

At Duke's request, an administrative assistant employed by OPD contacted Arch Wireless. After verifying that the City was the subscriber on the accounts, Arch Wireless provided the desired transcripts. Duke reviewed the transcripts and discovered that many of the messages sent and received on Quon's pager were not work related, and some were sexually explicit. Duke reported his findings to Scharf, who, along with Quon's immediate supervisor, reviewed the transcripts himself. After his review, Scharf referred the matter to OPD's internal affairs division for an investigation into whether Quon was violating OPD rules by pursuing personal matters while on duty.

The officer in charge of the internal affairs review was Sergeant Patrick McMahon. Before conducting a review, McMahon used Quon’s work schedule to redact the transcripts in order to eliminate any messages Quon sent while off duty. He then reviewed the content of the messages Quon sent during work hours. McMahon’s report noted that Quon sent or received 456 messages during work hours in the month of August 2002, of which no more than 57 were work related; he sent as many as 80 messages during a single day at work; and on an average workday, Quon sent or received 28 messages, of which only 3 were related to police business. The report concluded that Quon had violated OPD rules. Quon was allegedly disciplined.

The Fourth Amendment states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...” It is well settled that the Fourth Amendment’s protection extends beyond the sphere of criminal investigations. *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 530 (1967). “The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government,” without regard to whether the government actor is investigating crime or performing another function. *Skinner v. Railway Labor Executives’ Assn.*, 489 U.S. 602, 613–614 (1989). The Fourth Amendment applies as well when the Government acts in its capacity as an employer. *Treasury Employees v. Von Raab*, 489 U.S. 656, 665 (1989).

ie business school

93%
OF MIM STUDENTS ARE
WORKING IN THEIR SECTOR 3 MONTHS
FOLLOWING GRADUATION

MASTER IN MANAGEMENT

- STUDY IN THE CENTER OF MADRID AND TAKE ADVANTAGE OF THE UNIQUE OPPORTUNITIES THAT THE CAPITAL OF SPAIN OFFERS
- PROPEL YOUR EDUCATION BY EARNING A DOUBLE DEGREE THAT BEST SUITS YOUR PROFESSIONAL GOALS
- STUDY A SEMESTER ABROAD AND BECOME A GLOBAL CITIZEN WITH THE BEYOND BORDERS EXPERIENCE

Length: 10 MONTHS
Av. Experience: 1 YEAR
Language: ENGLISH / SPANISH
Format: FULL-TIME
Intakes: SEPT / FEB

5 SPECIALIZATIONS
PERSONALIZE YOUR PROGRAM

#10 WORLDWIDE
MASTER IN MANAGEMENT
FINANCIAL TIMES

55 NATIONALITIES
IN CLASS

www.ie.edu/master-management | mim.admissions@ie.edu | [f](#) [t](#) [i](#) Follow us on IE MIM Experience

Before turning to the reasonableness of the search, it is instructive to note the parties' disagreement over whether Quon had a reasonable expectation of privacy. The record does establish that OPD, at the outset, made it clear that pager messages were not considered private. The City's Computer Policy stated that "[u]sers should have no expectation of privacy or confidentiality when using" City computers. App. to Pet. for Cert. 152a. Chief Scharf's memo and Duke's statements made clear that this official policy extended to text messaging. The disagreement, at least as respondents see the case, is over whether Duke's later statements overrode the official policy. Respondents contend that because Duke told Quon that an audit would be unnecessary if Quon paid for the overage, Quon reasonably could expect that the contents of his messages would remain private.

From OPD's perspective, the fact that Quon likely had only a limited privacy expectation, with boundaries that we need not here explore, lessened the risk that the review would intrude on highly private details of Quon's life. OPD's audit of messages on Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his home phone line, would have been. That the search did reveal intimate details of Quon's life does not make it unreasonable, for under the circumstances a reasonable employer would not expect that such a review would intrude on such matters. The search was permissible in its scope.

Because the search was reasonable, petitioners did not violate respondents' Fourth Amendment rights, and the court below erred by concluding otherwise. The judgment of the Court of Appeals for the Ninth Circuit is reversed, and the case is remanded for further proceedings consistent with this opinion.

1.10 STATE CONSTITUTIONS

State constitutions are a second main source of privacy law. Typically, a state will adopt language from selective provisions of the U.S. Constitution (such as the search and seizure provisions of the Fourth Amendment) to provide an implied protection of invasion of privacy by a state government. However, many state constitutions go further and protect an individual's privacy from the state through legislation in such areas as privileged communications between a cleric and a penitent, wiretapping, and health information regarding prescriptions dispensed. For example, under Michigan Compiled Laws (MCL) 600.2162, in a civil or criminal lawsuit or administrative proceeding, a spouse cannot be a witness against another spouse without consent of the defendant spouse.

1.11 KEY TERMS

Administrative agency rules and actions	Fourth Amendment	Privacy zones
Appellate court	Fourteenth Amendment	Privacy zones
Case law	Implied right	Right to be left alone
Common law torts	Information privacy	Right to have personal physical space
Constitutional Amendments	International Association of Privacy Professionals (IAPP)	Right to keep personal information private
Derived right	Legal authority	Secondary authority
Federal court system	Legal right	State constitution
Federal statutes	Miranda warning	State court system
Fifth Amendment	Ninth Amendment	State statutes
First Amendment	Primary authority	Third Amendment
Five freedoms	Privacy	Trial court
		U.S. Constitution

1.12 CHAPTER DISCUSSION QUESTIONS

1. Define privacy.
2. What is the difference between primary and secondary authority?
3. What is the hierarchy of primary authority?
4. What are the five freedoms in the First Amendment of the Constitution? What do they mean to you?
5. How does the Ninth Amendment pertain to privacy rights?
6. Is there an expectation of privacy in the public realm? Why or why not?
7. Based on *Griswold v Connecticut*, does privacy extend outside your home?
8. What did Justice Douglas mean by the “penumbra of rights” in the *Griswold* case?
9. What is an implied legal right?
10. What is your definition of privacy? Is it similar or different to those discussed in this chapter?

1.13 ADDITIONAL LEARNING OPPORTUNITIES

1. The privacy rights of minors are different from adults because minors do not possess authority to make binding legal decisions. The U.S. Supreme Court in *T.L.O. v. New Jersey*, 469 U.S. 325 (1985), determined that public school officials could conduct a search of a student's purse for contraband without securing a search warrant in an effort to locate evidence the student had been smoking cigarettes at school. The Court held as long as the search was "reasonable," then the search was legal. How do you define reasonable? How did the Court define a reasonable search? See <http://www.uscourts.gov/educational-resources/educational-activities/new-jersey-v-tlo>.
2. It has been argued that there are two key threats to a person's privacy. These threats include other people and the government. Which is a greater threat? Why?



"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

1.14 TEST YOUR LEARNING

- 1) This Amendment to the U.S. Constitution is a safeguard against unreasonable searches and seizures:
 - a. 1st
 - b. 2nd
 - c. 3rd
 - d. 4th
 - e. 5th

- 2) A safe haven of privacy is known as a
 - a. Privacy zone
 - b. Privacy shelter
 - c. Privacy circle
 - d. Personal privacy
 - e. Public privacy

- 3) What is the difference between privacy and information privacy?
 - a. Information privacy is the right to be free from public attention.
 - b. Information privacy is the right to have control how your personal information is collected.
 - c. Information privacy is the right to have control how your personal information is used.
 - d. a and b
 - e. b and c
 - f. a and c

- 4) Is privacy a legal right?
 - a. Yes, because the U.S. Constitution explicitly states it is a legal right.
 - b. Yes, only because the federal courts have implied it is a legal right through the Amendments of the U.S. Constitution.
 - c. Yes, because it is included in the Constitution of all fifty states.
 - d. Yes, because it is included in the Preamble to the U.S. Constitution.

- 5) What federal case stated that a woman has a right to privacy as to an abortion?
 - a. *Griswold v. Connecticut*
 - b. *Katz v. United States*
 - c. *Meyer v. Nebraska*
 - d. *NAACP v. Alabama*
 - e. *Pierce v. Society of Sisters*
 - f. *Roe v. Wade*

- 6) Which of the following freedoms are protected by the First Amendment?
 - a. Assembly
 - b. Petition
 - c. Press
 - d. Religion
 - e. Speech

- 7) What is the strongest legal authority upon which a court can rely when rendering a decision?
 - a. U.S. Court cases
 - b. Federal Statutes
 - c. U.S. Constitution
 - d. Federal Court Rules
 - e. Treaties between the U.S. and other countries

- 8) What Constitutional Amendment protects an individual's right against self-incrimination?
 - a. First
 - b. Second
 - c. Third
 - d. Fourth
 - e. Fifth

- 9) True or False? If a person is incarcerated in prison, prison officials have the right to take a DNA sample of that person to place in a national DNA database.

- 10) True or False? Person A is growing marijuana plants in her basement. Her local police department drives by her home and uses a thermal imaging device to detect a large amount of heat in her basement. The police use the thermal imaging information to secure a warrant to search the property. This is a legal use of the information acquired from the device.

Test Your Learning answers are located in the Appendix.

2 PRIVACY TORTS

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

- Define a common law tort;
- Understand the elements of the four main categories of privacy torts;
- Provide examples of each of the privacy torts; and
- Apply the elements of each tort to contemporary examples.

2.1 OVERVIEW

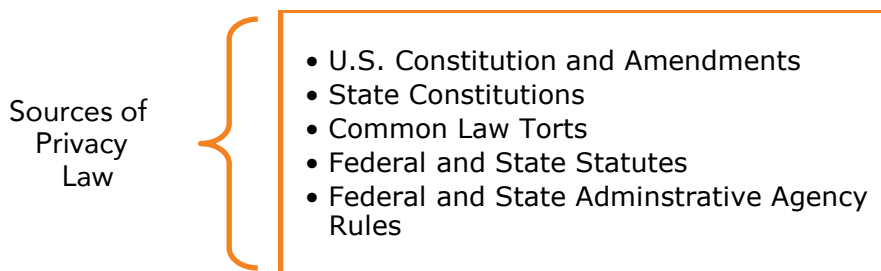


Figure 2-1

Excellent Economics and Business programmes at:



university of groningen



“The perfect start of a successful, international career.”

CLICK HERE
to discover why both socially and academically the University of Groningen is one of the best places for a student to be

www.rug.nl/feb/education

In Chapter One, you were introduced to the five sources of privacy law. You learned that the strongest and most important source of privacy law is the Amendments to the United States Constitution, and in particular the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. You also learned that the right to privacy is not expressly stated in the Constitution or the Amendments. Instead, through its court rulings addressing the question of privacy, the U.S. Supreme Court has determined there exists a penumbral or implied right of privacy from intrusion through the Constitutional Amendments.

You were also briefly introduced to a second source of privacy law: state constitutions. A State Constitution will often look like the Federal Constitution in design, in that it will define the structure of its government. State Constitutions' protections can expand an individual's privacy rights beyond the protections implied from the United States Constitution. For example, the National Conference of State Legislatures has reported that ten states provide an explicit right to privacy in their constitutions: "Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington."⁴⁸ Additionally, states can expand privacy rights through state legislation.

2.2 COMMON LAW TORTS

A third source of privacy law is the **common law**. Privacy is a type of **tort** under the common law. Torts are not **crimes**,⁴⁹ but instead involve **civil disputes** between two or more parties. A tort is an act or omission of one person against another that causes harm or injury. An injury in the context of a tort does not, however, always mean a physical injury, but could consist of an economic or monetary injury. Privacy disputes often result in litigation, which results in money damages being awarded to the prevailing party. Alternatively, as a part of a settlement, a court may order a party to refrain from acting in a manner harmful to the other party.

Figure 2-2 provides examples of the types of cases heard by the federal courts and the state courts. Privacy tort litigation is most often a state civil dispute.

The Federal Court System	The State Court System
<ul style="list-style-type: none"> • Cases that deal with the constitutionality of a law; • Cases involving the laws and treaties of the U.S.; • Cases involving ambassadors and public ministers; • Disputes between two or more states; • Admiralty law; • Bankruptcy; and • Habeas corpus issues. 	<ul style="list-style-type: none"> • Most criminal cases, probate (involving wills and estates) • Most contract cases, tort cases (personal injuries), family law (marriages, divorces, adoptions), etc. <p>State courts are the final arbiters of state laws and constitutions. Their interpretation of federal law or the U.S. Constitution may be appealed to the U.S. Supreme Court. The Supreme Court may choose to hear or not to hear such cases.</p>

Figure 2-2: Types of cases heard by federal and state courts – Materials in the public domain⁵⁰

2.3 DAMAGES

Damages that can be awarded in tort actions include **compensatory**, **punitive** (called **exemplary**⁵¹ in some jurisdictions), and **nominal**. Compensatory damages are intended to make a party “whole” for the losses caused due to injury by another party. There are two types of compensatory damages: special and general. **Special damages** are intended to provide reimbursement for economic losses. **General damages** reimburse for or non-economic injury, such as pain and suffering. Punitive damages are intended to punish the offending party “when the defendant’s (*i.e.* person being sued) willful acts were malicious, violent, oppressive, fraudulent, wanton, or grossly reckless.”⁵² Nominal damages consist of a small money award, such as \$1.00, when a party that has been harmed (perhaps morally or ethically) was unable to prove a financial loss.

	Purpose	Examples
Compensatory (Special)	Make the victim whole as if the harm had not occurred	Reimbursement for medical expenses, lost wages, repair or replacement of property
Compensatory (General)	These are difficult to calculate, and vary by circumstance	Payment for pain and suffering, loss of consortium, loss of reputation
Punitive/Exemplary	Intended to punish the defendant	Involves a financial award, typically awarded by a jury
Nominal	The court agrees a party has been wronged, but there are no proven compensable damages	Usually a nominal award
Statutory	Where the law designates the amount of damages to be awarded	Harm to a party may not be required

Table 2-1: A comparison of damages available in a tort action

American online LIGS University

is currently enrolling in the
Interactive Online **BBA, MBA, MSc,**
DBA and PhD programs:

- ▶ enroll **by September 30th, 2014** and
- ▶ **save up to 16%** on the tuition!
- ▶ pay in 10 installments / 2 years
- ▶ Interactive **Online** education
- ▶ visit www.ligsuniversity.com to find out more!

Note: LIGS University is not accredited by any nationally recognized accrediting agency listed by the US Secretary of Education. [More info here.](#)



2.4 TYPES OF PRIVACY TORTS

Legal tradition as well as court decisions group privacy torts into four classifications. These include:

1. Unreasonable **intrusion upon the seclusion** of others (often called intrusion);
2. **Misappropriation** and use of another person’s name or likeness;
3. **Public disclosure of private facts** that cause unreasonable publicity; and
4. Publicly and unreasonably placing a person in a **false light**.⁵³

The four groupings were originally created by William Prosser, a leading scholar on torts,⁵⁴ who crafted these definitions based on custom and prior court rulings called “common law.” These classifications are also described in a scholarly treatise known as the *Restatement of Torts, Second*. This text, published by the American Law Institute, compiled these privacy principles in a series of consecutive, numerical legal concepts citing to secondary sources of legal authority.⁵⁵

2.5 PUBLIC VERSUS PRIVATE

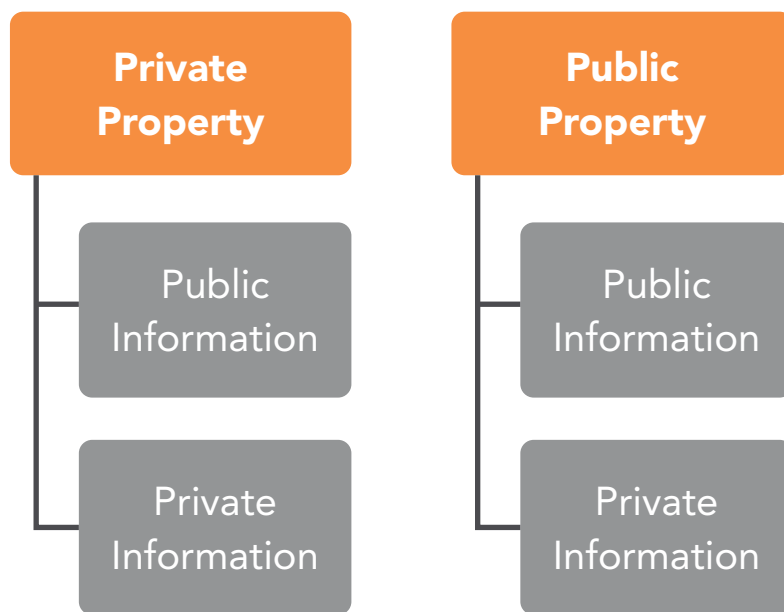


Figure 2-3: Illustration of public and private information as to property rights



Figure 2-4: Public notice of private property – Used with permission⁵⁶

Based on the four types of privacy torts, privacy violations may be viewed in terms of location: public places and private places. Additionally, privacy may be viewed from the perspective of the types of activity being engaged. In other words, based on the activity and location, there are different expectations of privacy. For example, there is an expectation of privacy inside your home, generally regardless of the type of activity. However, outside the front door, there is little to no expectation of privacy, as others might be able to see you from perhaps a neighbor’s yard or from a public street.

As we review each of the four types of privacy torts, please keep theses aspects in mind.

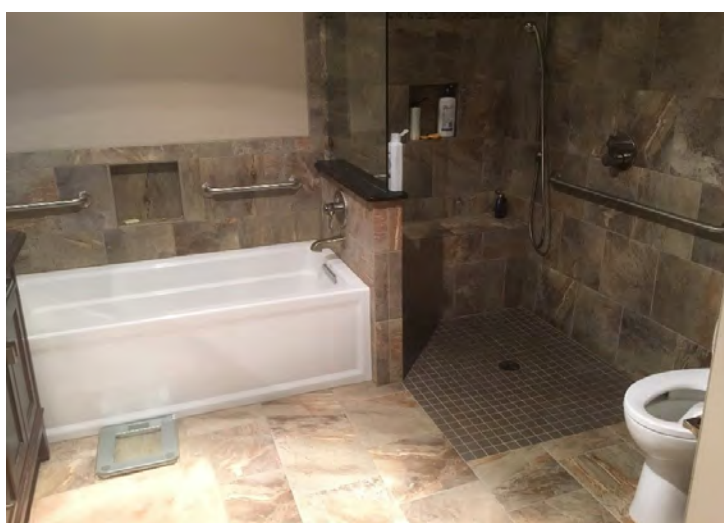


Figure 2-5: Is there an expectation of privacy in a home bathroom?
– Used with permission⁵⁷



Figure 2-6: Is there an expectation of privacy in a public restroom? – Used with permission⁵⁸

DON'T EAT YELLOW SNOW


What will your advice be?

Some advice just states the obvious. But to give the kind of advice that's going to make a real difference to your clients you've got to listen critically, dig beneath the surface, challenge assumptions and be credible and confident enough to make suggestions right from day one. At Grant Thornton you've got to be ready to kick start a career right at the heart of business.

Sound like you? Here's our advice: visit GrantThornton.ca/careers/students

Scan here to learn more about a career with Grant Thornton.



 **Grant Thornton**
An instinct for growth™

© Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd



Figure 2-7: Is there an expectation of privacy if your garbage is placed at the end of a driveway in public view on a public road? Used with permission⁵⁹



Figure 2-8: Is there an expectation of privacy walking down on a public street? – Used with permission⁶⁰

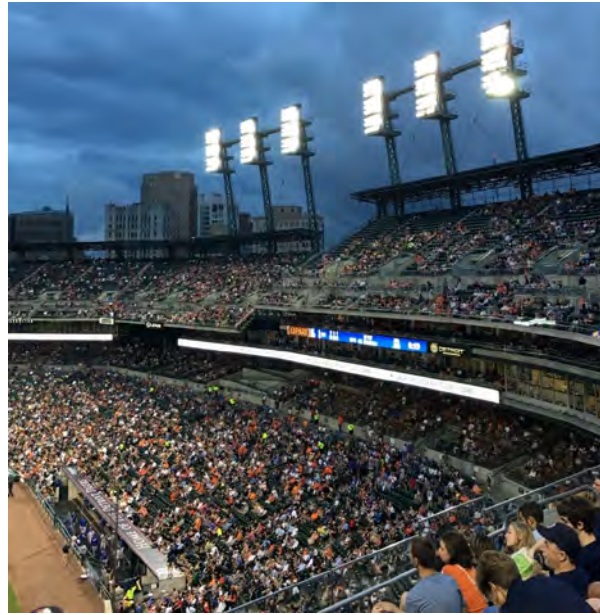


Figure 2-9: Is there an expectation of privacy while attending a public sports event? – Used with permission⁶¹



Figure 2-10: Is there an expectation of privacy while attending a public event at which the President of the United States is present? – Used with permission⁶²

2.6 TORT CATEGORY ONE: INTRUSION

Intrusion is defined by the *Restatement of the Law, Second, Torts, §652* as “(o)ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”⁶³

In other words, for a violation to exist, there must be 1) an intentional intrusion, 2) upon a person’s physical privacy or information deemed private, and 3) the intrusion must be **highly** (emphasis added) offensive to the average person. Take for example the illustration below. The photo to the left is a picture of a person’s front door taken from a public street. However, look at the photo on the right. If the homeowner’s front door to the home is open, can you simply walk inside uninvited? If you do so, you have intentionally entered the person’s home without permission. These actions and this intrusion would be highly offensive to most people, and in this scenario, a tort violation of intrusion would have been committed.

.....Alcatel-Lucent 

www.alcatel-lucent.com/careers

What if you could build your future and create the future?

One generation's transformation is the next's status quo. In the near future, people may soon think it's strange that devices ever had to be "plugged in." To obtain that status, there needs to be "The Shift".



Figure 2-11 and

Figure 2-12: Used with permission

2.7 DEFENSES TO INTRUSION

If a party is sued for intrusion,⁶⁴ there are several legal approaches or defenses the person or organization can invoke. To begin, let’s go back to Figure 2-12. Assume in Figure 2-12 the residence in the photo is located on a busy public street in suburban Chicago. Seeing the open door, a neighbor calls the police believing someone has broken into the home. In this example, if the police were to enter the home, this would be an appropriate law enforcement response called **customary or common usage**. Customary or common usage would be a defense to an allegation of intrusion in these circumstances.

A second defense is that the intrusion took place in public. For example, we have already discussed the concept of private versus public expectations of privacy. Assume someone photographs you attending a sports event with a colleague when you are supposedly working at home, and posts the photograph on the Internet, which is then published by a local newspaper. When your employer sees the photo, you are immediately fired because of your dishonesty. You could not sue the photographer or the newspaper for intrusion, as there is no expectation of privacy in public.

In the instance of intrusion into information, a third defense is *voluntarily* sharing of information. Last, a fourth defense may be waiver, if a party waived their right to keep information private.

The above examples do not include the element of technology, but rather concern property, whether real or intangible information, in a traditional sense. However, hidden surveillance cameras in a home, or an unauthorized webcam recording could easily be applied the traditional definition of intrusion. For example, in 2010 a Pennsylvania School District was charged with intrusion because webcam recording software was installed and active on laptops given to students for home use. The case known as *Robbins, et al v Lower Merion School District, et al*, was a federal case⁶⁵ filed in the Pennsylvania Eastern District Court that alleged a breach of privacy based on intrusion due to “indiscriminate remote activation of the webcams incorporated into each laptop...”⁶⁶ Not only were the parents not advised of the remote viewing, but anything within the range of the webcam could be recorded. Below is an excerpt that includes the invasion of privacy allegations against the School District.

**COUNT VII – INVASION OF
PRIVACY: PENNSYLVANIA COMMON LAW¹**

74. Plaintiffs repeat and re-allege each and every preceding allegation as if fully set forth herein.

75. At all times material hereto, and pursuant to the common law of Pennsylvania, Plaintiffs and all members of the Class had a reasonable expectation of privacy with respect to the operation of the webcams complained of.

76. Plaintiffs and Class members were never informed of the School District’s capability and practice of remotely activating the webcams complained of.

77. As the laptops at issue were routinely used by the students, their friends and family members while at home, it is believed and therefore averred that many of the webcam images captured and/or intercepted consist of minors and/or their parents in compromising or embarrassing positions, including, but not limited to, in various stages of dress or undress.

Figure 2-13: Image from the *Robbins, et al v Lower Merion School District, et al* court case – Materials in the public domain⁶⁷

Among other things, the families asked for compensatory and punitive damages.⁶⁸ The case was eventually settled for \$610,000.⁶⁹

2.8 TORT CATEGORY TWO: MISAPPROPRIATION

Misappropriation involves appropriating someone's picture, name, or likeness without permission for either a personal or commercial benefit,⁷⁰ that damages the person's reputation or causes personal embarrassment. The use of a person's name or likeness must be purposeful. The person is not required to be famous for misappropriation to occur. Take for example the case of *Bullard v. MRA Holding, LLC*.⁷¹ This Georgia Supreme Court case involved a then 14-year old girl who, while exercising poor judgment, exposed her breasts during a Spring vacation in Panama City, Florida. The incident was videotaped and reproduced in a *Girls Gone Wild* video, which "features young, and sometimes underage, women in states of partial or total nudity, and sometimes performing more explicit sex acts."⁷² As detailed in court documents:

Plaintiff is a private citizen who, when 14 years old and while walking down a main thoroughfare during spring break in Panama City, Florida, bared her breasts to two men whom she had just met and who had asked to see her "boobs." With plaintiff's knowledge, one of the men made a video recording of this exposure. In doing so, plaintiff joined in what has apparently become a spring break tradition among some young women. They bare their breasts or otherwise expose themselves to a male onlooker, who is often armed with a video camera, and who, in return, hands the girls some inexpensive, plastic beads.⁷³



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

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

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

www.mastersopenday.nl

Defendants later used the videoed and photographic image of plaintiff in its videos: *Girls Gone Wild*, *College Girls Exposed*, *Volumes 1 and 2*. Plaintiff's baring of her breasts was shown in an approximately five second clip on the video. Her still-image was also put on the cover of the video box, with her breasts blocked out by the inscription, "Get Educated!" Given her cover status on the video box, plaintiff's image was repeatedly broadcast on television advertisements, as well as on the Internet. From these widespread advertisements, plaintiff was recognized by students and teachers at her school, as well as other members of her community. She suffered great humiliation and distress from the extensive airing of her indiscretion.⁷⁴

The Georgia Supreme Court held the elements of misappropriation existed in this case including: "(1) appropriation of another's name and likeness whether such likeness was a photograph or another reproduction of the person's likeness, (2) without consent, and (3) the appropriation was for the financial gain of the appropriator."⁷⁵

Restatement of the Law, Second, Torts, §652

Appropriation of Name or Likeness

One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.

Figure 2-14: Elements of Misappropriation as stated in the *Restatement Torts, Second*⁷⁶

In most states, there are different legal standards for a private person as contrasted with someone in the public light (or a celebrity) whose identity has been misappropriated. This is because a celebrity's likeness has a monetary value. So, different legal implications exist when using the likeness of a private person for an advertising campaign and using the likeness of a well-known actress. For example, suppose a college student dresses up for a Halloween party appearing to look like the late singer Michael Jackson. The student wears a costume similar to Mr. Jackson's signature sunglasses with a silver glove on his right hand. Factors weighing against misappropriation might include that 1) the student does not look like Michael Jackson, 2) people know he is not Michael Jackson, and 3) he is not using the late singer's actual image for profit.

As suggested in the above example, misappropriation can apply to celebrities who are deceased. A person's likeness is a property right transferrable to another or held by the estate of the deceased. Indeed, there is often value to the estate of deceased celebrities,⁷⁷ including their voice and image.

Another example of misappropriation that led to litigation involved the actress Katherine Heigl. The actress, well known for her acting on the ABC television show *Grey’s Anatomy*, was leaving the Duane Reade pharmacy and photographed without her consent. (Duane Reade markets itself as the “the largest and most recognized drug store chain in the New York Metropolitan area serving customers since 1960.”⁷⁸) It is common for celebrities to be photographed in public particularly in New York City. However, the pharmacy distributed Heigl’s photo on Twitter® and Facebook® to promote their retail establishment. Heigl did not give her consent or permission for the pharmacy to use her likeness to promote their company. She subsequently sued⁷⁹ in the federal District Court in New York, and the case was dismissed later in 2014 in an undisclosed settlement.

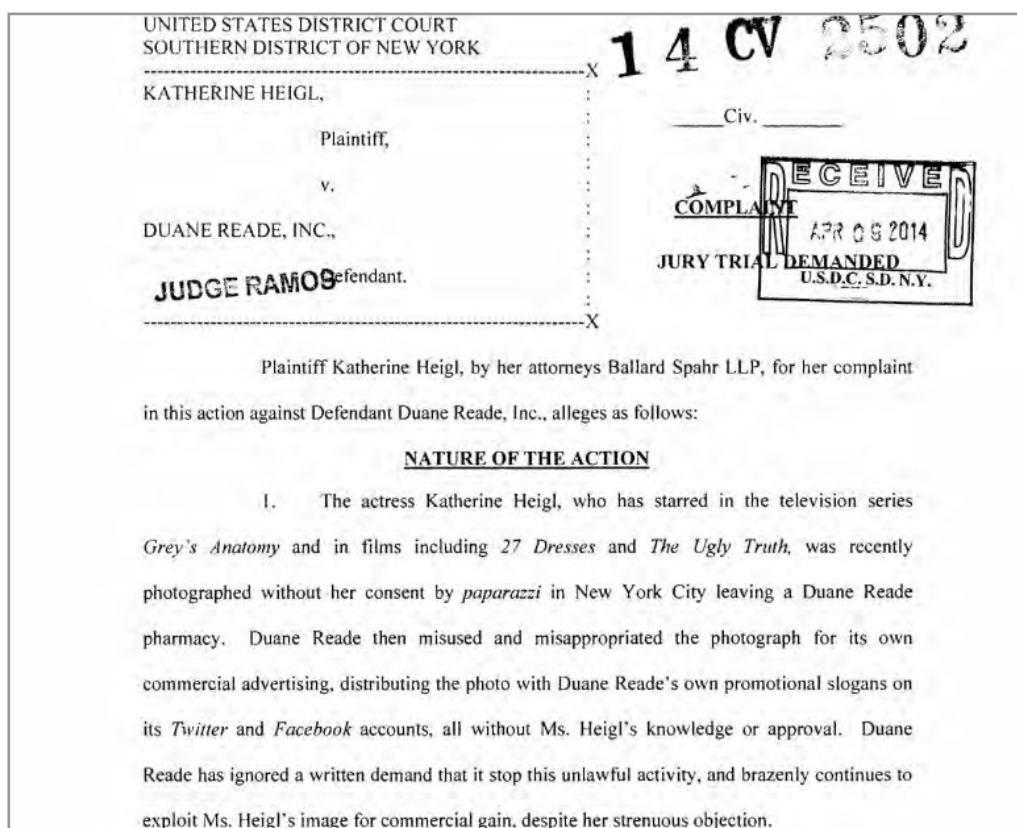


Figure 2-15: Page One of the Heigl Complaint filed against Duane Reade, Inc. in the United States District Court Southern Division – Materials in the public domain⁸⁰



Figure 2-16: Photo from Exhibit E in the Heigl Complaint – Materials in the public domain⁸¹

2.9 DEFENSES TO MISAPPROPRIATION

As with intrusion, defenses include consent, that information was shared with permission, that a party waived their right to their image or likeness, or the information was newsworthy.

BI NORWEGIAN BUSINESS SCHOOL

EFMD EQUIS ACCREDITED

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

www.bi.edu/master

2.10 CATEGORY THREE: PUBLIC DISCLOSURE OF PRIVATE FACTS

The third tort is the “public disclosure of private facts.” This tort requires:

- 1) the sharing of private information a person would not want disseminated;
- 2) that is disseminated to others;
- 3) that has had no legitimate public interest, and
- 4) that the disclosure would be offensive to a reasonable person.

Additionally, the information cannot be available through a public source, such as those described in the table below.

Criminal History	Marriage License	Court Dockets
Vehicles Owned	Real Estate Owned	Sex Offender Registry
FOIA Requests	Voter Registration	Death Certificate

Table 2-2: Examples of Public Information⁸²

Private facts would be information that a person would not want shared to the public. This could be the fact that the person has a disease or health condition.

Let’s use as an example the health of former and now deceased CEO, Steve Jobs, who was diagnosed in 2003 with a rare form of pancreatic cancer. He shared that information publically in 2004. However, in 2009 Jobs’ appearance was deteriorating, as he had lost substantial weight, causing speculation on this health status.⁸³ The company refused to answer questions about Jobs’ health, saying his medical information was a private matter.⁸⁴ Some would argue that the health of the CEO of one of America’s largest corporations was newsworthy, as Jobs was Apple’s top executive, and if he stepped down this could potentially have affected the financial value of the company. This was information significant to an investor, and arguably a legitimate concern to Apple shareholders, but was it a reasonable *public* concern? One could make an argument either way. However, health information has traditionally been deemed private, and more importantly has been protected by a variety of federal laws including the Health Insurance Portability and Accountability Act.⁸⁵

Courts often have distinguished between the privacy rights of an average person versus a public figure and determined that those in the public eye, have less privacy rights than the average person.

2.11 DEFENSES TO PUBLIC DISCLOSURE OF FALSE FACTS

As noted above, information that is newsworthy and has a “legitimate public concern,” or is publically available is a defense to the distribution of private information. Additionally, a person could consent to the sharing of the private information. Because the requirements for each of the torts discussed in this chapter are state specific, it is also possible that there be a requirement of reckless or intentional sharing of the information.

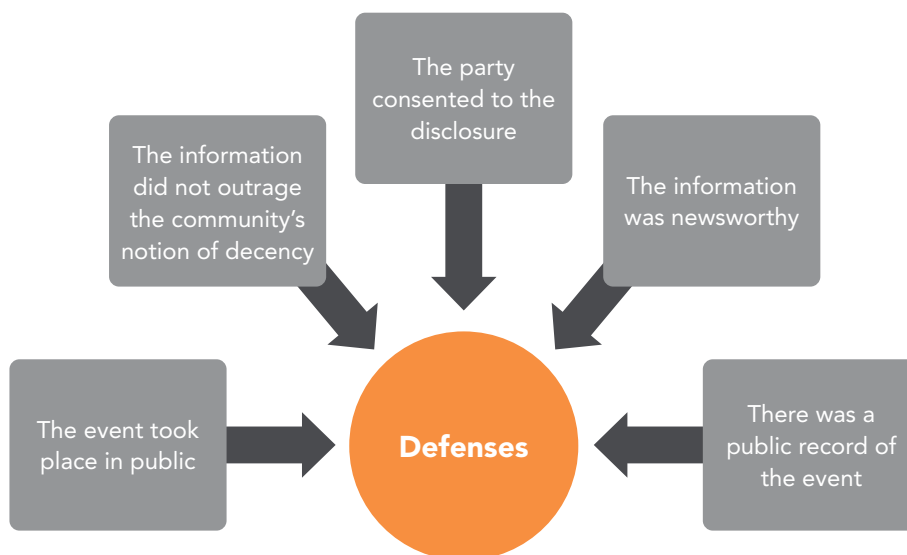


Figure 2-17: Defenses to Public Disclosure of False Facts

2.12 CATEGORY FOUR: FALSE LIGHT

Our last tort is “publicity placing another in a false light.” This means falsely connecting a person to an immoral, illegal, or embarrassing situation causing damage to their reputation.

Restatement of Torts 2d, §652e defines this tort as: “(a) the false light would be highly offensive to a reasonable person, and (b) 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.”⁸⁶

For example, suppose someone takes a photo of your female friend while at a company picnic. Then the photographer takes the photo and using image modification software, places your friend’s face on a nude photo. The modified picture is then posted on the Internet with your friend’s name. Not only did your friend not give permission for anyone to associate her name with the modified photo, the photographer acted in a reckless manner and intentionally associated the photo with her name. The actions of the photographer would be “highly offensive to a reasonable person,” meeting all the requirements for a false light tort action.

Here is another example. Suppose a person goes online to place a negative review about a hotel. The review states that the hotel is cockroach infested and that there were body secretions on the bed sheets and pillow cases. However, in reality, the author made the review because he is angered by the fact the hotel recently laid off his wife, and in spite he knowingly posts the false information. His intent is to cause economic harm to the hotel and create a downturn in reservations. Are the elements for false light present? The first question is whether the actions are highly offensive to a reasonable person? The second question is whether the author acted in reckless disregard to the falsity of the information in the post. Assuming the answer to both questions is “yes,” the author could be sued for damages by the hotel for placing the business in a “false light.”

However, not all states recognize this tort. For example, the State of Virginia does not support a false light claim, nor does New York or Ohio. Check the laws in your own state for the various types of privacy claims covered by the state law.

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



2.13 DEFENSES TO FALSE LIGHT

Key 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; or
- Consent.

2.14 KEY TERMS

Civil dispute Common law Compensatory damages Crime Customary or common usage Damages	Exemplary Damages False light General Damages Intrusion upon seclusion Misappropriation Nominal Damages	Public disclosure of private facts Punitive Damages <i>Restatement of Torts, Second</i> Special Damages Torts
--	--	---

2.15 CHAPTER DISCUSSION QUESTIONS

1. What is a tort? How does a tort differ from a crime?
2. What are compensatory damages? Provide an example.
3. What is the difference between special damages and general damages?
4. Describe an example in which it would be appropriate for a jury to award punitive damages.
5. What is an unreasonable intrusion upon the seclusion of others?
6. How close to a person’s name or likeness must there exist to be a valid cause of misappropriation?
7. What is an example of placing a person in false light?
8. Why does it matter if a tort takes place in a private versus a public setting?
9. List three defenses to the public disclosure of private facts.
10. List five sources of public information that can be used as a defense in a privacy tort case.

2.16 ADDITIONAL LEARNING OPPORTUNITIES

1. The Electronic Privacy Information Center (www.epic.org), describes itself as “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.” Its website includes information on emerging privacy issues. Based on your exploration of the website, what emerging issues do you see in the area of privacy tort law?

2. Video voyeurism occurs when someone is videotaped in a private setting. This type of privacy violation has become more common with technology. Check out this example of video voyeurism at www.hollandlawfirm.com/pdf/media_Video%20Voyeurism%20Case.pdf and read about the trial challenges in proving this type of case.
3. The Gawker Media Group was sued in the past year by former professional wrestler Hulk Hogan. Gawker published a video of Hogan having intercourse with the wife of a radio celebrity. Starting with <https://www.wsj.com/articles/gawker-and-hulk-hogan-in-settlement-talks-over-invasion-of-privacy-case-1470617756>, determine whether you agree or disagree with the outcome of the case.

2.17 TEST YOUR LEARNING

- 1) What is a tort?
 - a. It is a type of civil dispute between two or more private parties.
 - b. It is a type of criminal dispute brought by the government against someone who has violated a law.
 - c. It is a type of criminal dispute between two or more private parties.
 - d. It is a type of civil dispute brought by the government against someone who has violated a law.
- 2) Brian accesses Karol's brokerage account without her permission. He has access to the password because Karol had written it down in a notebook. Brian simply views the information, and he does not attempt to access any funds from the account. He is simply curious to know how much money Karol has. Brian's actions could constitute which of the following?
 - a. False light
 - b. Intrusion
 - c. Misappropriation
 - d. Negligence
 - e. Public disclosure of private facts
- 3) These types of damages are intended to punish a party for their actions:
 - a. Compensatory
 - b. Nominal
 - c. Punitive
 - d. Statutory
 - e. None of the above

- 4) Dale sues Harper for spreading a false rumor that she has spread a sexually contagious disease with several partners. Dale can sue Harper for:
 - a. Intrusion upon seclusion
 - b. Misappropriation of another person's name or likeness
 - c. Public disclosure of private facts
 - d. Publicly and unreasonably placing a person in a false light

- 5) Alex sues Harper for spreading information (that is true) that she has spread a sexually contagious disease with several partners. Alex can sue Harper for:
 - a. Intrusion upon seclusion
 - b. Misappropriation of another person's name or likeness
 - c. Public disclosure of private facts
 - d. Publicly and unreasonably placing a person in a false light

- 6) An action for intrusion upon seclusion focuses on the manner in which information is obtained, and not the fact it was shared or published.
 - a. True; the method obtaining the information must be objectionable to a reasonable person
 - b. False; it is irrelevant what method is used to obtain the information



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

- 7) Which of the following would be the public disclosure of private facts?
- Information about a person's divorce and how assets were distributed
 - Information about a person's criminal conviction
 - Information about a person's blood disease
 - Information about a person's driving record
 - Information about a person's professional license
- 8) Coats 'R Us placed a billboard on a major intersection in Arlington, VA with an image showing the President of the United States wearing one of its coats. The photo was taken by a White House photographer. The billboard implied the President endorsed the product. This is an example of
- Intrusion upon seclusion
 - Misappropriation of another person's name or likeness
 - Public disclosure of private facts
 - Publicly and unreasonably placing a person in a false light
 - None of the above
- 9) Invasion of privacy involves the
- Public disclosure of personal information
 - Public disclosure of embarrassing private facts
 - Disclosure to one person of personal information
 - Disclosure to one person of embarrassing private facts
- 10) Define public disclosure of private facts.
- There must be a public disclosure of one or more private facts.
 - There must be a public disclosure of one or more private facts which would be offensive and objectionable.
 - There must be a public disclosure of one or more private facts which would be offensive and objectionable to the reasonable person.
 - There must be a public disclosure of one or more private facts which would be offensive and objectionable to the reasonable person, which is not of legitimate public concern.
 - These are definitions for intrusion by seclusion, and not the public disclosure of private facts.

Test Your Learning answers are located in the Appendix.

3 PRIVACY AT HOME

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

- Explain the legal definition of a home;
- Describe the privacy protections an individual has inside and outside the home;
- Explain how the Fourth Amendment protects a person's privacy in the home;
- Describe the privacy issues using the Internet of Things (IoT); and
- Discuss the special privacy rights given to parents and guardians to protect private information about their children.



Figure 3-1: Used with permission⁸⁷

3.1 DEFINITION OF A HOME

As previously mentioned, the law recognizes privacy within a person's home. Under the Fourth Amendment, a person has the expectation that their home will be "free from governmental intrusion."⁸⁸ However, to understand the expectations of privacy within the home, the first question is to ask: how does the law define a **home**? For example, is an apartment a home? Is a home only the physical space within the building? If your home is a house, does your home include the yard surrounding the physical house? What about the driveway to a house?

3.2 MAPP V. OHIO⁸⁹

The Fourth Amendment of the U.S. Constitution is a basis for **reasonable expectations of privacy** in various aspects of the home. For example, it is well established under the federal Constitution that a homeowner has the right to expect privacy (as well as their family members and any guests) within the physical space of a person's home. Law enforcement officers cannot simply break down your front door and indiscriminately search your home. Intrusion into a home requires **probable cause** and a **search warrant** from an appropriate court.⁹⁰ Warrants must be specific. They must provide in detail where the search will take place and what items the police are intending to seize. It would be unusual that police would receive a general warrant without this type of detail. The illustration below provides a short overview of the *Mapp v. Ohio*, 367 U.S. 643 (1961), which is still cited today as providing the standard for the search of a person's home.

TURN TO THE EXPERTS FOR **SUBSCRIPTION** CONSULTANCY

Subscribe is one of the leading companies in Europe when it comes to innovation and business development within subscription businesses.

We innovate new subscription business models or improve existing ones. We do business reviews of existing subscription businesses and we develop acquisition and retention strategies.

Learn more at [linkedin.com/company/subscribe](https://www.linkedin.com/company/subscribe) or contact Managing Director Morten Suhr Hansen at mha@subscribe.dk

SUBSCR✓**BE** - to the future

Decision Date: June 19, 1961

Background:

The case originated in Cleveland, Ohio, when police officers forced their way into Dollree Mapp's house without a proper search warrant. Police believed that Mapp was harboring a suspected bomber, and demanded entry. No suspect was found, but police discovered a trunk of obscene pictures in Mapp's basement. Mapp was arrested for possessing the pictures, and was convicted in an Ohio court. Mapp argued that her Fourth Amendment rights had been violated by the search, and eventually took her appeal to United States Supreme Court. At the time of the case unlawfully seized evidence was banned from federal courts but not state courts.



Decision:

The U.S. Supreme Court ruled in a 5-3 vote in favor of Mapp. The high court said evidence seized unlawfully, without a search warrant, could not be used in criminal prosecutions in state courts.

Figure 3-2: Materials in the public domain⁹¹

One question to consider is whether technology affects the ruling in *Mapp*. Take for example, the case of *Kyllo v. United States*, 533 U.S. 27 (2001)⁹² discussed briefly in Chapter One. In *Kyllo*, law enforcement had reason to believe that the defendant was growing marijuana in his home. Marijuana plants require consistent heat and light, so the police determined that they could use thermal imaging, an infrared radiation technology, to identify heat sources in Kyllo's home.

As noted in the Court's decision:

The imager converts radiation into images based on relative warmth – black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images. The scan of Kyllo's home took only a few minutes and was performed from the passenger seat of Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex.⁹³

The U.S. Supreme Court ruled that a search warrant was required to use this technology "that would previously have been unknowable without physical intrusion."⁹⁴

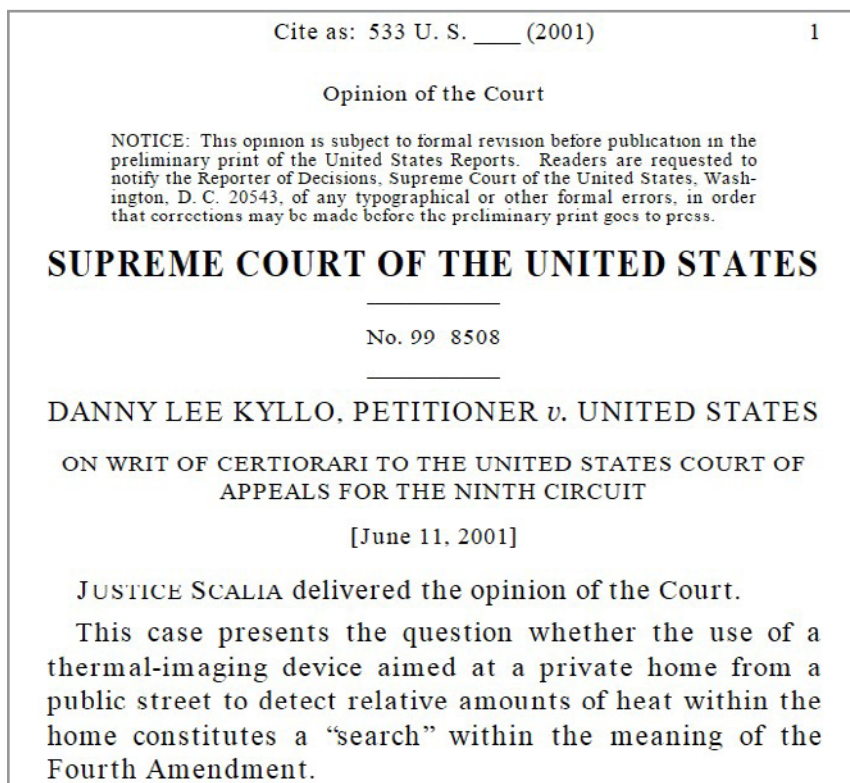


Figure 3-3: Materials in the public domain⁹⁵

3.3 CURTILAGE

At the beginning of this chapter, several questions were posed to define a home. One of those questions asked was whether the definition of your home included your front and back yard, as well as your driveway. This takes us to the topic of **curtilage**. The U.S. Supreme Court in *Oliver v. United States*, 466 U.S. 170 (1984)⁹⁶ has defined this concept to be “the area around the home to which the activity of home life extends.”⁹⁷ Under the *Oliver* standard, it would seem logical that a front porch would be considered a part of house. However, in the case of *Florida v. Jardines*, 569 US ___, 133 S.Ct. 1409 (2013)⁹⁸ this concept was questioned.

Jardines involved a “drug sniffing dog Franky, who was accompanying his handler after police received a tip about an alleged marijuana growing activity inside a house. Franky was on the house’s porch when he alerted police to the presence of marijuana. The Supreme Court ruled in a 5–4 decision that Franky’s sniff was a Fourth Amendment violation,”⁹⁹ and a search warrant was needed before the canine’s skills could be deployed.

(Slip Opinion) OCTOBER TERM, 2012 1

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

FLORIDA v. JARDINES

CERTIORARI TO THE SUPREME COURT OF FLORIDA

No. 11–564. Argued October 31, 2012—Decided March 26, 2013

Police took a drug-sniffing dog to Jardines’ front porch, where the dog gave a positive alert for narcotics. Based on the alert, the officers obtained a warrant for a search, which revealed marijuana plants; Jardines was charged with trafficking in cannabis. The Supreme Court of Florida approved the trial court’s decision to suppress the evidence, holding that the officers had engaged in a Fourth Amendment search unsupported by probable cause.

Figure 3-4: Materials in the public domain¹⁰⁰



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

3.4 SAMPLE SCENARIOS



Figure 3-5: The main house – Used with permission¹⁰¹



Figure 3-6: A building adjacent to the main house, used as a greenhouse – Used with permission¹⁰²

Let’s further explore the concept of curtilage by looking at Figures 3-5 and 3-6. Figure 3-5 is a photograph of a home. Figure 3-6 is a picture of a greenhouse located in very close physical proximity to the home. If you look closely at the bottom right side of Figure 3-5, you will see the greenhouse in very close proximity to the residence.

Scenario 1: Suppose that the police secure a search warrant for the greenhouse (Figure 3-6), that omits any mention of the home. Can the law enforcement officials enter a person's house? Generally, the answer is no. Officers executing a search warrant must limit their search to the area described in the warrant. If a warrant specifically authorizes a search of a greenhouse, officers would probably not be within their legal right to search the home.

Scenario 2: Again assume that the search warrant is for the greenhouse only. Look at Figure 3-5. Suppose the officers take a ladder from the greenhouse, prop it against the home and peek in through the second floor windows. They see no evidence of criminal activity in "plain view," however, they decide to enter the home and search. Again, this would not be a legal search.

Scenario 3: Suppose the police search the greenhouse and, while doing so, hear screaming from the home. They run into the home and find one person holding a bloody knife, and a second person severely injured. Can the officers enter the home without a warrant? Yes, these would be exigent circumstances as the screaming would give officers probable cause because a person was in eminent physical danger.

Scenario 4: Using the same facts in Scenario 3, assume the officers were wearing a body cam, and the local news station has requested copies of the video to play on their evening news. Are the police required to share the footage? The answer to this question is based on several factors. Since the footage is a part of an ongoing criminal investigation, it is considered evidence and a part of the criminal case. This means the police agency would generally not be required to disclose the footage. Second, there is an issue of privacy of the victims, so many law enforcement departments, even after a case is closed, will have internal policies that limit the public sharing of the information.

Keep in mind that a warrant is not required if any of the following exist:

- 1) "the consent of the resident,
- 2) if an illegal substance or activity in the house is in 'plain view' of the officers,
- 3) a search incident to a lawful arrest,
- 4) or an emergency where the police have been called to assist."¹⁰³

However, in today's world, most everyone has a cell phone that includes a plethora of personal data. So, what about cell phone data? Is a warrant required? See the case of *Riley v California*¹⁰⁴ below for the U.S. Supreme Court's view on the question.

Note: This case involved two parties, Riley and Wurie.

***Riley v. California*, 573 U.S. ____, 134 S.Ct. 2473 (2014)**¹⁰⁵

Opinion by Justice Roberts, Jr.

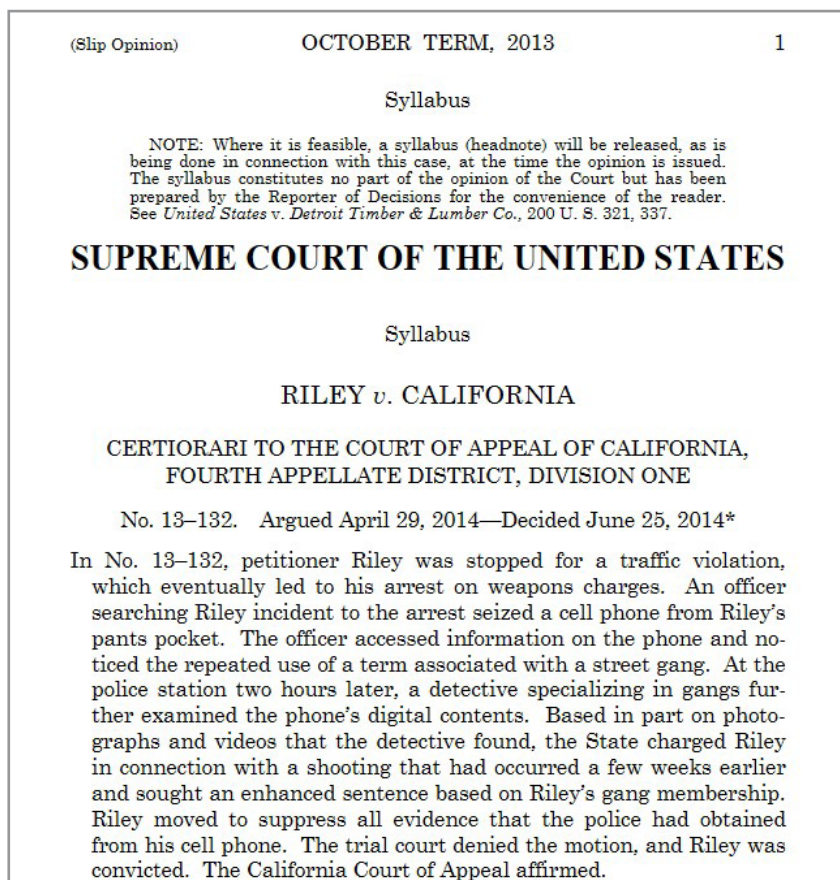


Figure 3-7: Materials in the public domain¹⁰⁶

In No. 13-212, respondent Wurie was arrested after police observed him participate in an apparent drug sale. At the police station, the officers seized a cell phone from Wurie’s person and noticed that the phone was receiving multiple calls from a source identified as “my house” on its external screen. The officers opened the phone, accessed its call log, determined the number associated with the “my house” label, and traced that number to what they suspected was Wurie’s apartment. They secured a search warrant and found drugs, a firearm and ammunition, and cash in the ensuing search. Wurie was then charged with drug and firearm offenses. He moved to suppress the evidence obtained from the search of the apartment. The District Court denied the motion, and Wurie was convicted.

Three related precedents govern the extent to which officers may search property found on or near an arrestee. *Chimel v. California*, 395 U.S. 752, requires that a search incident to arrest be limited to the area within the arrestee’s immediate control, and it is justified by the interests in officer safety and in preventing evidence destruction. In *United States v. Robinson*, 414 U.S. 218, the Court applied the *Chimel* analysis to a search of a cigarette pack found on the arrestee’s person. It held that the risks identified in *Chimel* are present in all custodial arrests, 414 U.S. at 235, even when there is no specific concern about the loss of evidence or the threat to officers in a particular case, *Id.* at 236. The trilogy concludes with *Arizona v. Gant*, 556 U.S. 332, which permits searches of a car when the arrestee is unsecured and within reaching distance of the passenger compartment, or when it is reasonable to believe that evidence of the crime of arrest might be found in the vehicle, *Id.* at 343.

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**

Cell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person. Notably, modern cell phones possess an immense storage capacity. Before cell phones, a search of a person was limited by physical realities and generally constituted only a narrow intrusion on privacy. But cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos. This has several interrelated privacy consequences. First, a cell phone collects in one place many distinct types of information that reveal much more in combination than any isolated record. Second, the phone's capacity allows even just one type of information to convey far more than previously possible. Third, data on the phone can date back for years. In addition, an element of pervasiveness characterizes cell phones but not physical records. A decade ago, officers might have occasionally stumbled across a highly personal item such as a diary, but today many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives.

It is true that this decision will have some impact on the ability of law enforcement to combat crime. But the Court's holding is not that the information on a cell phone is immune from search; it is that a warrant is generally required before a search. The warrant requirement is an important component of the Court's Fourth Amendment jurisprudence, and warrants may be obtained with increasing efficiency. In addition, although the search incident to arrest exception does not apply to cell phones, the continued availability of the exigent circumstances exception may give law enforcement a justification for a warrantless search in particular cases.

3.5 THE SKY

What, if any, area above your home is private? This question was addressed about 70 years ago by the U.S. Supreme Court. It is an unusual case that took place in the early 1940s that involved three elements: a farmer, chickens, and an airplane. The question in the case asked if there was any "reasonable expectation of privacy" in the sky above your home.



Figure 3-8: Used with permission¹⁰⁷

The Plaintiff was a chicken farmer by the name of Thomas Causby who sued the U.S. Army. Causby operated a thriving chicken farm, but at the beginning of World War II, the U.S. Army took over a local airport close to Causby's home. The airport was very busy with the arrival and departure of the military planes who upon takeoff flew low over the farmer's home. The noise and vibrations from the planes brought about enormous stress on Causby's chickens, causing them to fly into the chicken coop walls and eventually die. The U.S. Supreme Court¹⁰⁸ in reviewing the case, held that landowners own the sky above their homes up to 83 feet, as 83 feet was the lowest level of a flying plane at that time.

This e-book
is made with
SetaPDF



PDF components for PHP developers

www.setasign.com



Figure 3-9: Will the *Causby* case apply to the use of drones?¹⁰⁹ When does private airspace end and public airspace begin in the era of drones? The answer is unclear – Used with permission¹¹⁰

Causby was a civil case and damages were appropriately awarded to the farmer, but what about criminal investigations? In other words, can law enforcement officers use aerial surveillance as a tool for a criminal investigation. The answer to the question is interestingly “yes,” and a warrant is not required. This question actually came before the U.S. Supreme Court in 1989 in the case of *Florida v Riley*, 488 U.S. 445.¹¹¹ In *Riley*, police officials flew a helicopter over Riley’s home and observed from public airspace what appeared to be marijuana growing inside the defendant’s home. The Court held “(s)ince the FAA permits helicopters to fly below that limit, the helicopter here was not violating the law, and any member of the public or the police could legally have observed respondent’s greenhouse from that altitude.”¹¹²

Congress has given the power for the FAA to regulate air space over 500 feet.¹¹³ However, there is a void in the law who has the control in the air space gap between 83 and 500 feet.¹¹⁴ This will be an area of future legal challenges as the technology with drones becomes more sophisticated.

3.6 PRIVACY AND CHILDREN

As previously mentioned, the law recognizes the privacy of a person’s home. However, with respect to children, minors are placed in a special classification under the law,¹¹⁵ simply to protect them from harm. For example, children accused of crimes are handled by special courts that are closed to the public. Court records from these cases are also private and sealed. At home, the law protects children from parental or guardian neglect and requires children to be provided with the basic necessities of life.

Concerning children and technology, one main federal law relates to a child's privacy at home. This law is the **Children's Online Privacy Protection Act of 1998 (COPPA)**, 15 U.S.C. § 6501–6505. "COPPA imposes certain requirements on operators of websites or **online** services directed to **children** under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age."¹¹⁶ For parents and guardians this means that they can control personal information (See Figure 3-10) of their children under 13, and only they can give permission to share the personal information about their child.

Companies subject to COPPA must notify parents and guardians *directly* before they collect information about their children, and receive verifiable consent¹¹⁷ from the adult before any information is collected. The website must post a privacy policy online that details the collection and use of any personal information about children under thirteen, and the rights parents and guardians regarding the collection and use of the information. These organizations must also establish a plan and process for protecting and securing the information of these minors. Violators of the law are subject to civil penalties, and other enforcement actions. The **Federal Communications Commission (FCC)** has been charged by Congress with enforcing COPPA.

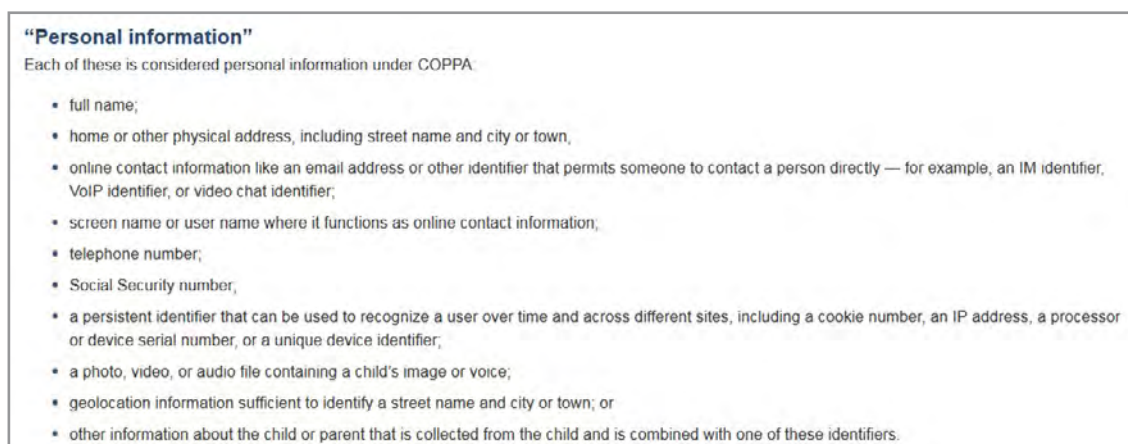


Figure 3-10: Federal Trade Commission Rules what is considered personal information – Materials in the public domain¹¹⁸

3.7 PRIVACY AND THE INTERNET OF THINGS

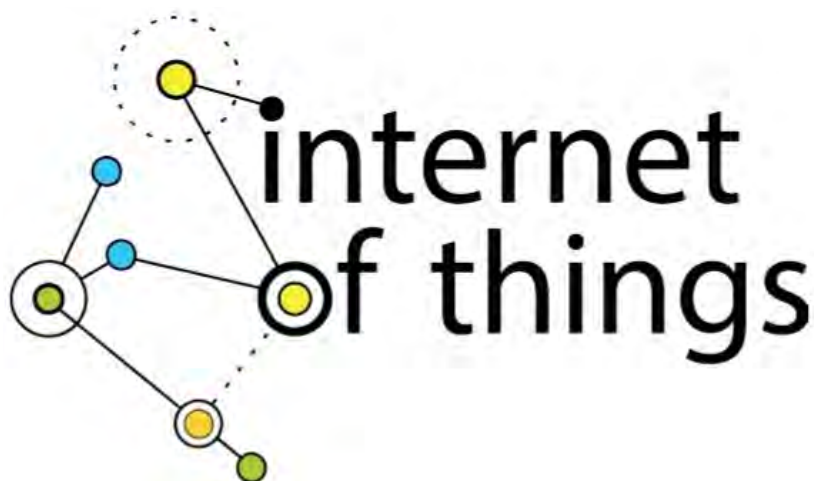


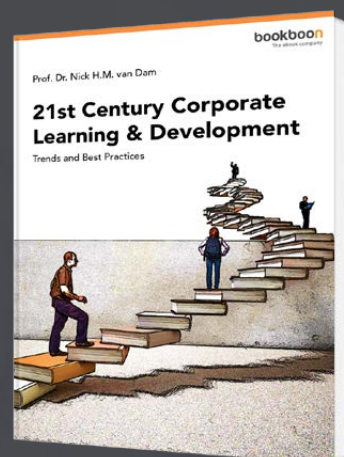
Figure 3-11: Materials in the public domain¹¹⁹

People need to be diligent with the technology in their home and be preemptive about privacy. Privacy issues can exist with any product that uses a network connection. Without appropriate security, these products can be hacked. Additionally, often times, data is stored by a manufacturer in a cloud environment, which may have inadequate security safeguards.

Free eBook on Learning & Development

By the Chief Learning Officer of McKinsey

[Download Now](#)



The **Internet of Things (IoT)** is a moniker given to “the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other).”¹²⁰ “This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. This also applies to components of machines. For example, a jet engine of an airplane or the drill of an oil rig both can operate with wireless connections.”¹²¹ The problem with these devices is that they can be subject to hacking if not properly secured.

Take for example, a wireless camera connected to a nursery. Without the proper precautions, the camera could be hacked, the baby could be kidnapped, and old footage could be placed in the camera feed giving the parents a false sense of security.

These types of privacy concerns are real. Suppose you are a diabetic patient on an insulin pump. It is critical that the correct amount of insulin be given to the patient. Hacking of the insulin pump¹²² could be medically disastrous to the patient. This is a true scenario as evidenced by a letter send to users of the OneTouch Ping system¹²³ manufactured and distributed by Johnson & Johnson. Similarly, the wireless Merlin@home™ cardiac monitoring system, has also been beset by claims of potential hacking and reprogramming of patient devices.¹²⁴ A software patch has been developed by the manufacturer and sent to all transmitter devices.



Figure 3-12: Used with permission¹²⁵

Similarly, assume you are wearing a fitness band communicating with a GPS system and location data stored on the cloud. Information can be inferred about your exercise and health habits. One common argument is insurance decisions and premium costs could be increased (or decreased) based on data found in fitness bands.¹²⁶

One of the latest technologies that has serious hacking implications surrounds driverless cars. There is evidence of several driverless cars being hacked, including a Jeep in 2015 that had a security flaw in the vehicles' entertainment system.¹²⁷

Consumers need to be prudent when making these types of purchases, and to question the security measures in place by the manufacturer to keep your data safe and private, by keeping equipment up to date and exercising strong password selection.

3.8 DATA BREACH NOTIFICATION

It is not unusual to read in the news about a breach of personal information. Small and large companies alike¹²⁸ have been targets of illegal hacking. **Breach notification laws** require an organization that has had a data breach to timely notify their customers in writing about the event.¹²⁹

Most **data breach** notification laws are state based. Typical state breach notification laws define the types of entities covered by the law, the data covered by a breach, the recipients of a notice of the breach, the timing the notice must be delivered, the penalties for non-compliance, and the right of a party to sue and recover damages.

Below is a sample email from Michigan State University¹³⁰ in East Lansing, Michigan sent in November 2016 to those who were previously notified of a data breach. The email and offered credit monitoring services for those whose information may have been compromised in that breach.

Dear [REDACTED]

Michigan State University is truly sorry for any inconvenience caused by this incident and we are committed to taking steps to protect your personal information.

You have automatic access to AllClear Identity Repair for the next 24 months through November 30, 2018; **there is no further action required on your part to receive this service.** If a problem arises, simply call 1-855-231-9331 and a dedicated investigator will assist you in restoring your identity to its accurate state.

You have requested AllClear Triple Bureau Opt-in Credit Monitoring service which includes credit monitoring and a \$1 million identity theft insurance policy. You may activate this service online at enroll.allclearid.com using the following redemption code(s):

[REDACTED]

Please note that certain features may require that you disclose other personal information to AllClear ID or take additional steps in order to activate your phone alerts.

For additional details or concerns about this incident, please visit:

www.msu.edu/datasecurity

We are truly sorry for any inconvenience this issue may have caused.

Figure 3-13: Used with permission¹³¹

www.sylvania.com

We do not reinvent the wheel we reinvent light.

Fascinating lighting offers an infinite spectrum of possibilities: Innovative technologies and new markets provide both opportunities and challenges. An environment in which your expertise is in high demand. Enjoy the supportive working atmosphere within our global group and benefit from international career paths. Implement sustainable ideas in close cooperation with other specialists and contribute to influencing our future. Come and join us in reinventing light every day.

Light is OSRAM

OSRAM SYLVANIA

On the federal side, both the Gramm-Leach-Bliley (GLBA) Act, 15 U.S.C. § 6801–6809 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 300gg, 29 U.S.C § 1181 et seq., 42 U.S.C § 1320d et seq. have data breach notification requirements.

3.9 KEY TERMS

Children Children’s Online Privacy Protection Act of 1998 Curtilage Data Breach Data Breach Notification Federal Communications Commission	Home Internet of Things Online Probable cause Reasonable expectation of privacy Search warrant Sky limits
---	---

3.10 CHAPTER DISCUSSION QUESTIONS

1. For privacy purposes, define a home.
2. What was the ruling in *Mapp v Ohio*? How does it relate to privacy?
3. What were the facts in *Kyllo*? How does the *Kyllo* ruling differ from *Mapp*?
4. What is curtilage? Is a pond on a person’s property curtilage? Why or why not?
5. What was the Court’s decision in the *Florida v. Jardines* case?
6. Do you agree with the result in Scenario 1? Why or why not?
7. Do you agree with the ed result in Scenario 4? Why or why not?
8. Is the *Causby* case still relevant today? Why or why not?
9. How does COPPA define personal information as it relates to children?
10. Give an example of three wireless devices used in a home that could have potential privacy issues?

3.11 ADDITIONAL LEARNING OPPORTUNITIES

1. Assume in the case of *Florida v. Riley*, 488 U.S. 445 (1989) that that a hot air balloon was flying over the residence of the parties who were working outdoors in their backyard. How do you predict the U.S. Supreme Court would rule on the privacy issues of the hot air balloon? Use the question “is there a reasonable expectation of privacy” as the standard of review.



Figure 3-14: Used with permission¹³²

2. Explore the Google Maps Street view lawsuit¹³³ involving a family by the name of the Borings, who objected to Google taking photos of their home and posting them on the Internet. The Court only awarded the Borings, nominal damages in the amount of \$1.00. Review the case at <http://www.pcmag.com/article2/0,2817,2373754,00.asp> and explain why the Court awarded only nominal damages.

3.12 TEST YOUR LEARNING

1. Under which Amendment has the U.S. Supreme Court recognized the privacy of a person's home?
 - a. 1st
 - b. 2nd
 - c. 3rd
 - d. 4th
 - e. 5th

2. Which one or more of the following would meet the definition of a home as defined by the U.S. Supreme Court?
 - a. Tent
 - b. Apartment
 - c. Boat
 - d. House
 - e. Dorm room

3. Does the “use of a thermal-imaging device aimed at a private house from a public street to detect relative amounts of heat within the home constitute a ‘search’”?
 - a. No
 - b. Yes
 - c. Maybe

4. Curtilage is
 - a. A garage attached to a home
 - b. A basement attached to a home
 - c. An attic attached to a home
 - d. A yard attached to a home
 - e. The roof of a home

5. A warrant to search a home is required under which of the following?
 - a. Consent of the occupant
 - b. An emergency situation
 - c. Drug paraphernalia in “plain view”
 - d. A neighbor’s hunch that illegal activity is taking place
 - e. A search incident to an arrest



Discover the truth at www.deloitte.ca/careers

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

6. The *Causby* case restricted private airspace to _____ feet.
 - a. 25
 - b. 50
 - c. 76
 - d. 83
 - e. 99

7. COPPA stands for the
 - a. Children's Online Privacy Protection Act
 - b. Child and Parents Online Privacy Personal Association
 - c. Children's Operational Privacy Protection Action
 - d. Childish Online Protection and Privacy Act

8. Under COPPA, parents and guardians can control personal information for minors under _____.
 - a. 8
 - b. 10
 - c. 12
 - d. 13
 - e. 14
 - f. 15

9. Under COPPA, which of the following is not personal information?
 - a. Favorite television show
 - b. Address
 - c. Hobby
 - d. Photo
 - e. Geolocation information

10. A data information breach law is typically
 - a. State based
 - b. Federal based
 - c. Both state and federal based

Test Your Learning answers are located in the Appendix.

4 PRIVACY OUTSIDE THE HOME

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

- Define an educational record and what personal information is protected;
- Describe HIPAA and explain who is required to protect health care information and what information is protected;
- Explain the rules for electronic medical records and how the information in those records must be protected;
- Explain requirements businesses must follow to protect credit information and the remedies available for correcting credit records; and
- Describe why and how voting records are protected.

4.1 OVERVIEW

Once a person walks out of their home, their privacy expectations change. This means that once in the public realm, your persona and activities are open to public view. However, certain federal laws have been enacted to protect some areas of a person's life and specific types of personal information. These areas include education and health care records, financial and credit information, and voting records.



Figure 4-1: Why are the faces of the children blocked?¹³⁴ – Used with permission¹³⁵

4.2 EDUCATION PRIVACY

The **Federal Family Educational Rights Privacy Act of 1974** or **FERPA**,¹³⁶ protects the educational records of students in both the K-12 educational systems and in college (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA is a federal law administered by the **Family Policy Compliance Office** in the **U.S. Department of Education (DOE)**.¹³⁷ It applies to educational institutions that receive federal funding. Private educational institutions are, therefore, not subject to FERPA requirements, as generally not being recipients of federal funds.

How to Read a Citation to a Federal Statute

Most information in this chapter is based on federal laws. Federal laws are cited in the form: 18 U.S.C. § 123. U.S.C. means the law is a part of the U.S. Code. The U.S. Code has 50 titles. 18 means that this law is in Title 18 of the U.S. Code. § 123 means the law is in section 123 of Title 18 of the U.S. Code.

The citation for FERPA is 20 U.S.C. § 1232g. This means this law is located in Title 20 of the U.S. Code in section 1232g. The U.S. Code does not use page numbers; instead it uses section numbers.

SIMPLY CLEVER

ŠKODA



We will turn your CV into an opportunity of a lifetime



Do you like cars? Would you like to be a part of a successful brand? We will appreciate and reward both your enthusiasm and talent. Send us your CV. You will be surprised where it can take you.

Send us your CV on www.employerforlife.com



The law gives parents/guardians (in the case of K-12 students), and college students the right to inspect, review and amend records, and restrict the disclosure of “**personally identifiable**” information. This means that information, such as grades, test scores, ID numbers, financial records, and disciplinary information is protected from release without the specific consent of the parent/guardian or the eligible student. All interested parties (*i.e.*, parents, guardians or students) must be advised of their FERPA rights by the school on a yearly basis.¹³⁸

Personally identifiable information, as defined in FERPA, includes, but is not limited to:

1. The student’s name;
2. The name of the student’s parent or other family members;
3. The address of the student or student’s family;
4. A personal identifier, such as the student’s Social Security Number, student number, or biometric record;
5. Other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name;
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty;
7. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
(34 CFR § 99.3)

Figure 4-2: Materials in the public domain¹³⁹

4.2.1 LEGITIMATE PUBLIC INTEREST

A basic rule is that an educational institution must have written permission from the appropriate party to disclose educational information. The law however provides for exceptions to this requirement for those with a “**legitimate educational**” interest, such as school officials¹⁴⁰ gathering data for research purposes. Other exceptions include the sharing of information:

- to authorized representatives of the Comptroller General of the United States, the Attorney General of the United States, the U.S. Secretary of Education, and State and local educational authorities for audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs;
- in connection with financial aid for which the student has applied or received;
- to state and local authorities pursuant to a State statute concerning the juvenile justice system and the system’s ability to effectively serve the student whose records are being disclosed;

- to organizations conducting studies for or on behalf of the school making the disclosure for the purposes of administering predictive tests, administering student aid programs, or improving instruction;
- to comply with a judicial order or a lawfully issued subpoena; and
- in connection with a health or safety emergency.¹⁴¹

However, under FERPA, schools are allowed to disclose *without written consent* directory information. “**Directory information**’ is defined as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Directory information could include information such as the student’s name, address, e-mail address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended, photograph, grade level (such as 11th grade or junior year), and enrollment status (full-time or part-time).”¹⁴²



Figure 4-3: Used with permission¹⁴³

The U.S. Department of Education (DOE) is the agency responsible for FERPA compliance. Individuals who feel their school or university has failed to be in compliance with FERPA should contact the DOE to file an appropriate complaint. The law only allows the DOE to pursue litigation and enforcement. In other words, individuals cannot sue a school or university for a FERPA violation.

About the Family Policy Compliance Office

The mission of the Family Policy Compliance Office (FPCO) is to meet the needs of the Department's primary customers--learners of all ages--by effectively implementing two laws that seek to ensure student and parental rights in education: the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA).

Parents and eligible students who need assistance or who wish to file a complaint under FERPA or PPRA should do so in writing to the Family Policy Compliance Office, sending pertinent information through the mail, concerning any allegations to the following address:

Family Policy Compliance Office
 U.S. Department of Education
 400 Maryland Avenue, SW
 Washington, D.C. 20202-5920
 Phone: 1-800-USA-LEARN (1-800-872-5327)

Figure 4-4: Materials the public domain¹⁴⁴




- The number 1 MOOC for Primary Education
- Free Digital Learning for Children 5-12
- 15 Million Children Reached

About e-Learning for Kids Established in 2004, e-Learning for Kids is a global nonprofit foundation dedicated to fun and free learning on the Internet for children ages 5 - 12 with courses in math, science, language arts, computers, health and environmental skills. Since 2005, more than 15 million children in over 190 countries have benefitted from eLessons provided by EFK! An all-volunteer staff consists of education and e-learning experts and business professionals from around the world committed to making difference. eLearning for Kids is actively seeking funding, volunteers, sponsors and courseware developers; get involved! For more information, please visit www.e-learningforkids.org.

4.2.2 THE OWASSO CASE

In 2002, the Owasso Independent School District in Oklahoma was sued (534 U.S. 426) by a parent for allowing peer grading of assignment or the scoring of tests by other students. The parent alleged this was a FERPA violation. “The issue before the Court in this case was whether allowing students to grade each other’s homework and tests as their teacher goes over the correct answers aloud in class was an educational record and violated the prohibition in the Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. 1232g, against the release, without parental consent, of students’ ‘education records’.”¹⁴⁵ The Court held in favor of the school district because “FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar, not individual assignments handled by many student graders in their separate classrooms.”¹⁴⁶ The case also reinforced under the FERPA statute that private lawsuits are an inappropriate remedy for FERPA enforcement and that the law allows the “Secretary of Education to cut off federal funding to educational institutions that violate the statute.”¹⁴⁷

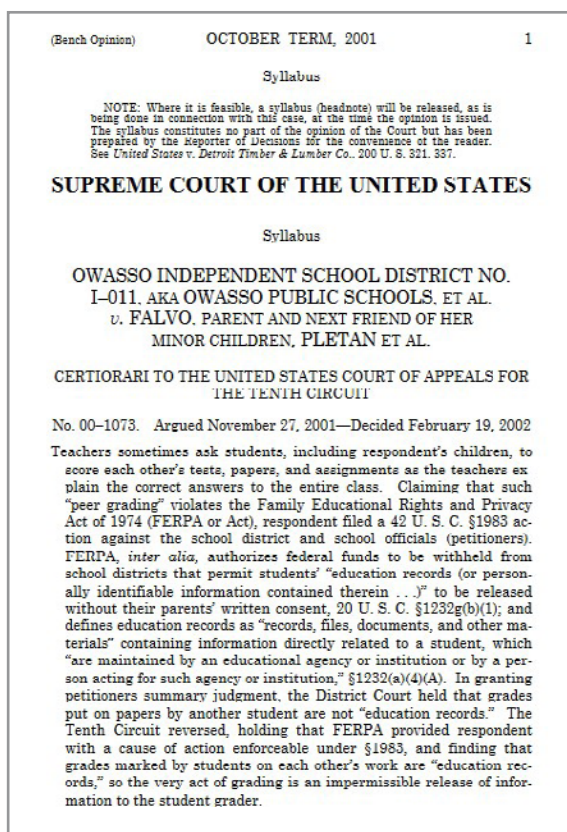


Figure 4-5: Materials in the public domain¹⁴⁸



Figure 4-6: Used with permission¹⁴⁹

4.3 HEALTH CARE PRIVACY

Health care privacy is covered by two federal laws. The first is the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, 42 U.S.C. § 300gg, 29 U.S.C § 1181 et seq., and 42 U.S.C. § 1320d et seq.,¹⁵⁰ which protects the privacy of patient records. The second is the **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009**, 42 U.S.C. § 1300 et seq.¹⁵¹ This law places requirements on physicians and hospitals to make all patient records electronic. Those not demonstrating “meaningful usage” of electronic records systems, will be subject to reduced Medicare reimbursement.¹⁵² Physicians not receiving Medicare reimbursement, do not have this requirement.



Are there penalties for providers who don't switch to electronic health records (EHR)?



If Medicare eligible professionals, or EPs, do not adopt and successfully demonstrate meaningful use of a certified electronic health record (EHR) technology by 2015, the EP's Medicare physician fee schedule amount for covered professional services will be adjusted down by 1% each year. The adjustment schedule is as follows:

- 2015—99% of Medicare physician fee schedule covered amount
- 2016—98 % of Medicare physician fee schedule covered amount
- 2017 and each subsequent year—97% of Medicare physician fee schedule covered amount

If less than 75% of EPs have become meaningful users of EHRs by 2018, the adjustment will change by 1% point each year to a maximum of 5%(95% of Medicare covered amount).

The Recovery Act allows for hardship exception from the payment adjustment in certain instances. The exemption must be renewed each year and will not be given for more than 5 years. More information on payment adjustments and the requirements to qualify for a hardship exemption will be provided in future rulemaking between now and the 2015 effective date.

Figure 4-7: Materials in the public domain¹⁵³

Cynthia | AXA Graduate

AXA Global Graduate Program

Find out more and apply

redefining / standards

4.3.1 THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

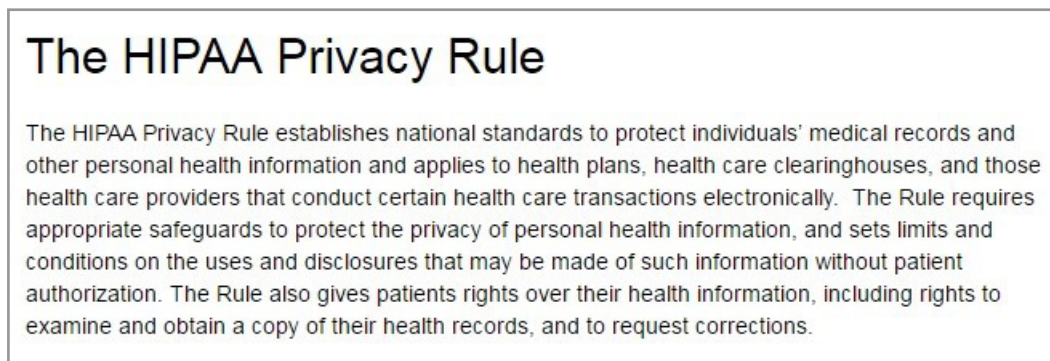


Figure 4-8: Materials in the public domain¹⁵⁴

HIPAA is a federal law that limits the sharing of patient health care records. It applies to health care providers, plans, and clearinghouse that transmit health information in an electronic form. These entities and individuals are required to follow certain safeguards to protect patient “**individually identifiable health information.**” The law also allows patients to determine who may access their records.

“Individually identifiable health information” includes information ‘that relates to

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,
- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.¹⁵⁵ Individually identifiable health information includes many common identifiers (*e.g.*, name, address, birth date, Social Security Number).’¹⁵⁶

“Your health care provider and health plan must give you a notice that tells you how they may use and share your health information. It must also include your health privacy rights. In most cases, you should receive the notice on your first visit to a provider or in the mail from your health plan. You can also ask for a copy at any time.”¹⁵⁷

What is in the Notice?

The notice must describe:

- How the Privacy Rule allows provider to use and disclose protected health information. It must also explain that your permission (authorization) is necessary before your health records are shared for any other reason
- The organization's duties to protect health information privacy
- Your privacy rights, including the right to complain to HHS and to the organization if you believe your privacy rights have been violated
- How to contact the organization for more information and to make a complaint




Figure 4-9: Materials in the public domain¹⁵⁸

Both civil and criminal penalties can be applied to violations. Civil penalties include a fine of \$100 to \$50,000 or more per violation with a yearly maximum of \$1,500,000. Criminal violators “may face a criminal penalty of up to \$50,000 and up to one-year imprisonment. The criminal penalties increase to \$100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to \$250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm. The U.S. Department of Justice is responsible for criminal prosecutions.”¹⁵⁹



Figure 4-10: Is the display of these photos of children placed in a dentist’s office a HIPAA violation? – Used with permission¹⁶⁰

4.3.2 HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT OF 2009

The Health Information Technology for Economic and Clinical Health Act of 2009 was enacted to promote the “**meaningful use of health information technology**”¹⁶¹ by health care professionals, and organizations. The U.S. Department of Health and Human Services, the responsible federal agency for this law, authorized its Office of National Coordinator (ONC) to set standards and manage compliance. Providers were offered financial incentives from 2015–2017¹⁶² to accelerate implementation of **electronic health care records (EHR)**.¹⁶³ HITECH adopters must also incorporate HIPAA requirements into their technology.

I joined MITAS because
I wanted **real responsibility**

The Graduate Programme
for Engineers and Geoscientists
www.discovermitas.com



Month 16

I was a construction supervisor in the North Sea advising and helping foremen solve problems

Real work
International opportunities
Three work placements





Figure 4-11: Materials in the public domain¹⁶⁴

The law imposes data breach notification requirements for unauthorized uses and disclosures of **protected health care information** or “**PHI**.”

“The regulations, developed by OCR (Office for Civil Rights¹⁶⁵), require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases in which a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.”¹⁶⁶

Breach Report Results							
Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information	
Fred's Stores of Tennessee, Incorporated	TN	Healthcare Provider	9624	09/29/2016	Theft	Laptop	
San Juan Oncology Associates	NM	Healthcare Provider	500	09/29/2016	Hacking/IT Incident	Network Server	
Central Ohio Urology Group, Inc.	OH	Healthcare Provider	300000	09/23/2016	Hacking/IT Incident	Network Server	
Hal Meadows, M.D.	CA	Healthcare Provider	8000	09/23/2016	Hacking/IT Incident	Desktop Computer	
Jennie Stuart Medical Center	KY	Healthcare Provider	1500	09/23/2016	Hacking/IT Incident	Network Server	
New Jersey Spine Center	NJ	Healthcare Provider	28000	09/22/2016	Hacking/IT Incident	Electronic Medical Record, Network Server	
USC Keck and Norris Hospitals	CA	Healthcare Provider	16000	09/21/2016	Hacking/IT Incident	Network Server	

Figure 4-12: Example of publicly available breach information available at the Department of Health and Human Services website – Materials in the public domain¹⁶⁷

Consider for example, a patient who visits their physician and is in need of antibiotic for a disease. The physician electronically transfers the prescription request to the local drug store. The physician is required to use due diligence to insure that the transfer of information be technologically secure to comply with the HIPAA privacy requirements.

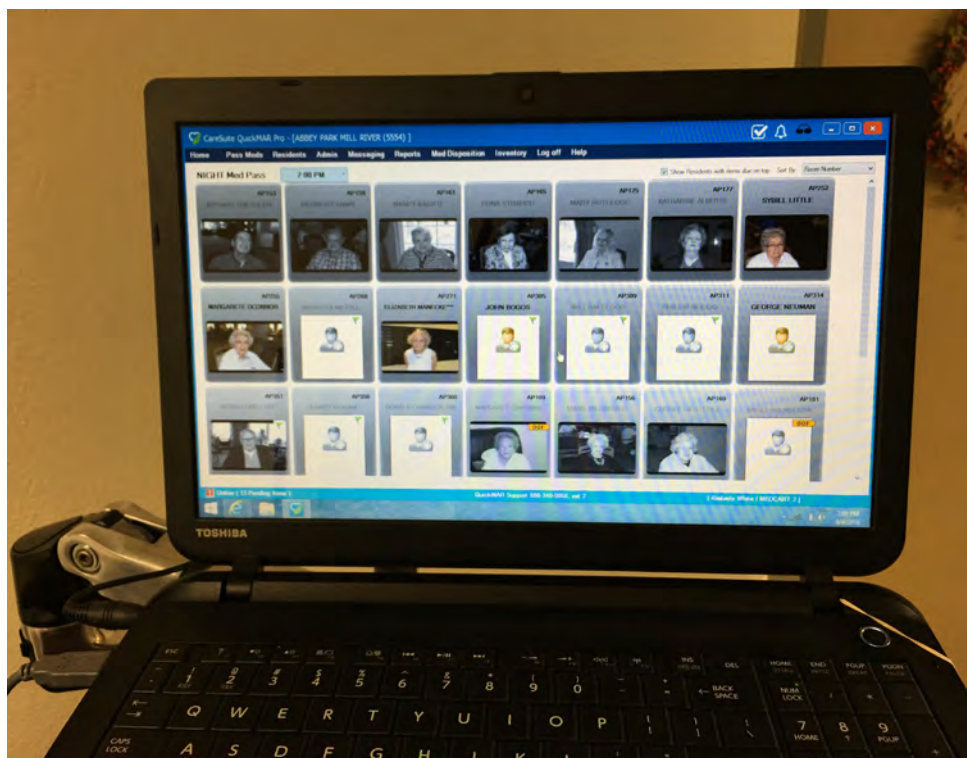


Figure 4-13: Example of client medical information observed in a hallway in an independent living facility serviced by a private personal assistant company
 Is this a HITECH or a HIPAA violation?¹⁶⁸ – Used with permission¹⁶⁹

4.4 FINANCIAL PRIVACY

Several federal laws protect consumer financial privacy. They include privacy protections with credit worthiness under the **Fair Credit Reporting Act of 1970 (FCRA)**, 15 U.S.C. § 1681 et seq.,¹⁷⁰ which allows a consumer to correct errors in their credit reports. **The Fair and Accurate Credit Transactions Act of 2003 (FACTA)**, 15 U.S.C. §1681c(g),¹⁷¹ includes provisions regarding identity theft, so consumers can make appropriate notifications credit reporting companies. Lastly, the **Financial Services Modernization Act of 1999** (commonly called Gramm-Leach-Bliley),¹⁷² requires companies to give notice of their privacy practices to consumers and allow individuals to opt out of the sharing of personal information.

4.4.1 THE FAIR CREDIT REPORTING ACT OF 1970 (FCRA)

The FCRA¹⁷³ is a federal law that protects consumer privacy, and restricts the ways that credit reporting agencies can use and report a person’s financial information. The reports created by credit agencies are used to evaluate a person’s credit worthiness.

The law also provides for a process for a person to request corrections to credit information. The Federal Trade Commission is the agency responsible for monitoring compliance with the FCRA and to ensure that consumer credit information is appropriately protected.

The main credit reporting agencies are Equifax[®],¹⁷⁴ TransUnion[®],¹⁷⁵ and Experian[®].¹⁷⁶ These three companies compile personal financial information and distribute primarily to companies interested in offering a person credit. Information gathered by credit agencies comes from data given to them by other financial institutions. Groups that contribute financial data to the reporting agencies include banks, credit card companies, mortgage brokers, and insurance companies.

Businesses must have a “**permissible purpose**,”¹⁷⁷ under FCRA to view reports; however, others such as employers (with your permission), collection agencies and insurance companies can access your credit information to use this information to do business with you.

ie business school

93%
OF MIM STUDENTS ARE
WORKING IN THEIR SECTOR 3 MONTHS
FOLLOWING GRADUATION

MASTER IN MANAGEMENT

- STUDY IN THE CENTER OF MADRID AND TAKE ADVANTAGE OF THE UNIQUE OPPORTUNITIES THAT THE CAPITAL OF SPAIN OFFERS
- PROPEL YOUR EDUCATION BY EARNING A DOUBLE DEGREE THAT BEST SUITS YOUR PROFESSIONAL GOALS
- STUDY A SEMESTER ABROAD AND BECOME A GLOBAL CITIZEN WITH THE BEYOND BORDERS EXPERIENCE

Length: 10 MONTHS
Av. Experience: 1 YEAR
Language: ENGLISH / SPANISH
Format: FULL-TIME
Intakes: SEPT / FEB

5 SPECIALIZATIONS
PERSONALIZE YOUR PROGRAM

#10 WORLDWIDE
MASTER IN MANAGEMENT
FINANCIAL TIMES

55 NATIONALITIES
IN CLASS

www.ie.edu/master-management | mim.admissions@ie.edu | [f](#) [t](#) [i](#) Follow us on IE MIM Experience

<p>You must be told if information in your file has been used against you.</p>	<p>Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information.</p>
<p>You have the right to know what is in your file.</p>	<p>You may request and obtain all the information about you in the files of a consumer reporting agency (your “file disclosure”). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if: a person has taken adverse action against you because of information in your credit report; you are the victim of identity theft and place a fraud alert in your file; your file contains inaccurate information as a result of fraud; you are on public assistance; you are unemployed but expect to apply for employment within 60 days. In addition, by September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies.</p>
<p>You have the right to ask for a credit score.</p>	<p>Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.</p>
<p>You have the right to dispute incomplete or inaccurate information.</p>	<p>If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous.</p>
<p>Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.</p>	<p>Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.</p>
<p>Consumer reporting agencies may not report outdated negative information.</p>	<p>In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.</p>

<p>Access to your file is limited.</p>	<p>A consumer reporting agency may provide information about you only to people with a valid need – usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.</p>
<p>You must give your consent for reports to be provided to employers.</p>	<p>A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry.</p>
<p>You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.</p>	<p>Unsolicited “prescreened” offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).</p>
<p>You may seek damages from violators.</p>	<p>If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.</p>
<p>Identity theft victims and active duty military personnel have additional rights.</p>	<p>For more information, visit www.ftc.gov/credit.</p>
<p>States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.</p>	

Table 4-1: A summary of consumer rights under FCRA – Materials in the public domain¹⁷⁸

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Date]

Complaint Department
[Company Name]
[Street Address]
[City, State, Zip Code]

Dear Sir or Madam:

I am writing to dispute the following information in my file. I have circled the items I dispute on the attached copy of the report I received.

This item [identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.] is [inaccurate or incomplete] because [describe what is inaccurate or incomplete and why]. I am requesting that the item be removed [or request another specific change] to correct the information.

Enclosed are copies of [use this sentence if applicable and describe any enclosed documentation, such as payment records and court documents] supporting my position. Please reinvestigate this [these] matter[s] and [delete or correct] the disputed item[s] as soon as possible.

Sincerely,
Your name

Enclosures: [List what you are enclosing.]

Figure 4-14: Sample dispute letter to a credit agency – Materials in the public domain¹⁷⁹



"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

4.4.2 THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 (FACTA)



Figure 4-15: Materials in the public domain¹⁸⁰

This law, enacted in 2003 amended the Fair Credit Reporting Act and added “provisions designed to prevent and mitigate identity theft.”¹⁸¹ One key provision of the law allows a person to place a **fraud alert** in their credit files. To take advantage of this law, the victim must:

- 1) contact one of the three major credit reporting bureaus;
- 2) advise the company you have been a victim of identity theft and request them to place a fraud alert on your file;
- 3) confirm the company will contact the other two credit reporting agencies (this is a requirement of FACTA).¹⁸²

A fraud alert will stay in the consumer’s file for 90 days. It can be extended an additional 90 days per the consumer’s request. Victims of identity theft should also monitor their credit reports for any unusual activity.¹⁸³

Mrs. Gray is an 80-year old woman living in an independent living facility called Amy Parke. Mrs. Gray is very sharp mentally, but physically she needs assistance with personal grooming. The Amy Parke where she lives has a contract with Helpers ‘R Us and Mrs. Gray receives Services from Helpers. Mrs. Gray’s daughter Colleen manages her finances. One day she was balancing her mother’s checking account when she noticed some missing checks. One month later, a check for \$2000.00 is written on Mrs. Gray’s account and Colleen’s signature was forged. Under FACTA, who can place a fraud alert? Mrs. Gray, Colleen, or both parties.

An **extended fraud alert**¹⁸⁴ is also an option for consumers that will be active for seven years. To complete this process, the victim must complete the identify theft form available through the FTC, and send this report to all three of the credit agencies, and request the extended fraud alert.¹⁸⁵

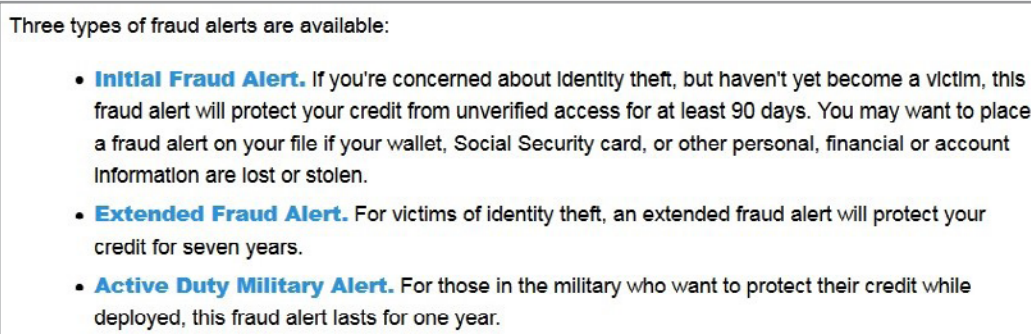


Figure 4-16: Materials in the public domain¹⁸⁶

In contrast to a credit alert is a **security or credit freeze**.¹⁸⁷ All consumers, not only those crime victims, have the option to place a security or credit freeze on their accounts with the credit reporting companies. This restricts the sharing of credit information to potential lenders and credit card companies (with the exception of existing creditors and court orders and subpoenas.) The consumer will have to actively remove the freeze from the credit agency if requesting credit.

4.4.3 THE FINANCIAL SERVICES MODERNIZATION ACT OF 1999

The Financial Services Modernization Act of 1999 is more well known as **Gramm-Leach-Bliley Act (GLBA)**.¹⁸⁸ The law focuses on customer financial institutions and customer safeguards, but law includes many privacy protections for consumers. “Financial institutions covered by the Gramm-Leach-Bliley Act must tell their customers about their information-sharing practices and explain to customers their right to ‘opt out’ if they don’t want their information shared with certain third parties.”¹⁸⁹ This opting out is often referred to as the **Privacy Rule**. Under GLBA financial institutions must send a written notice (unless a customer has opted to receive electronic information) to its customers on a yearly basis detailing its privacy policies and reminding the consumer on their option to “opt out” of sharing personal information.

Examples of financial institutions covered under the law include companies involved in debt collecting, offering real estate settlement services, lending companies, companies providing financial, investment or economic advisory services, or those servicing loans.¹⁹⁰

Examples of "consumer" relationships:

- cashing a check with a check-cashing company
- making a wire transfer
- applying for a loan, whether or not you actually obtain the loan

Figure 4-17: Materials in the public domain¹⁹¹

The Privacy Rule covers consumer’s “**nonpublic personal information (NPI)**”. NPI is “personally identifiable financial information” that a financial institution collects about an individual in connection with providing a financial product or service.”¹⁹² This means public real estate records such as mortgages, deeds and tax record would not meet the definition of NPI. Nor would information found on websites, social media accounts or newspapers be NPI. On the other hand, a listing of credit card holders for a major retailer would be considered NPI under the law. In other words, the retailer might share its customer lists with an affiliate company, who in turn could solicit those customers by sending them marketing emails or a catalog through the mail.

Excellent Economics and Business programmes at:



**university of
 groningen**



“The perfect start
 of a successful,
 international career.”

CLICK HERE
 to discover why both socially
 and academically the University
 of Groningen is one of the best
 places for a student to be

www.rug.nl/feb/education

The law also has enacted a **Safeguards Rule**.¹⁹³ This rule requires that financial institutions indicate in their annual privacy notice how personal information will be kept confidential and safeguarded.

Another rule under the Financial Services Modernization Act of 1999 is called the **Red Flags Rule**. It requires that covered financial institutions have a written Identity Theft Prevention Program “designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations.”¹⁹⁴



Figure 4-18: Materials in the public domain¹⁹⁵

What is a red flag? This is account activity that suggests identity theft is taking place on a customer account. The red flag could consist of a significant difference in spending patterns, or incorrect verification information from a consumer. Customers cannot sue for non-compliance; the Federal Trade Commission is the authorized party to start actions for compliance issues. Violations include monetary civil penalties and injunctive relief with a maximum of \$3500 per violation.¹⁹⁶

4.5 VOTING PRIVACY

Central to democracy in the United States, is the integrity of the voting process. Although under the **Voting Rights Act**, 42 U.S.C. § 1973 et. seq.¹⁹⁷ your actual vote is private, there is public data collection and availability of registration information that includes the voter’s name, address, possible political preferences, and in which elections a person voted. Voter registration data is commonly used by candidates and political parties to educate and promote candidates to voters. Additionally, the Federal Elections Commission regulations require presidential campaigns to publish the lists of individual donors of over \$100.¹⁹⁸

Each individual state will also have its own voter privacy law that protects your privacy with local and state elections.



Figure 4-19: Sample Voter Information Available Through Public Records

4.6 THE CHILDREN’S INTERNET PROTECTION ACT (CIPA)

“**The Children’s Internet Protection Act (CIPA)** (27 U.S.C. § 1701 et. seq.) was enacted by Congress in 2000 to address concerns about children’s access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries.”¹⁹⁹

Applicable libraries must have an Internet blocking and filtering program for pictures that are harmful to minors such as child pornography and other photos deemed to be obscene.

The “protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors).”²⁰⁰ The library must also monitor the online use of minors and have an education program for minors about appropriate online behavior.

4.7 KEY TERMS

Children’s Internet Protection Act CIPA Directory Information EHR Electronic health care records Extended fraud alert FACTA Fair Credit Reporting Act of 1970 The Fair and Accurate Credit Transactions Act of 2003 Family Policy Compliance Office FCRA Federal Family Educational Rights Privacy Act of 1974	FERPA Financial Services Modernization Act of 1999 Fraud alert GLBA Gramm-Leach-Bliley Act Health Insurance Portability and Accountability Act of 1996 Health Information Technology for Economic and Clinical Health Act of 2009 HIPAA Individually identifiable health information Legitimate educational interest	Meaningful use of health information technology HITECH NPI Nonpublic personal information Permissible purpose Personally identifiable information PHI Privacy Rule Red Flags Rule Protected health care information Safeguards Rule Security or credit freeze Voting Rights Act
---	---	---

4.8 CHAPTER DISCUSSION QUESTIONS

1. Under FERPA, what is an educational record?
2. What federal agency has responsibility for FERPA compliance?
3. Health care privacy is covered by what two laws? How are they different?
4. What is the HIPAA Privacy Rule?
5. Give two examples of individually identifiable health information.
6. What is the difference between the Fair Credit Reporting Act of 1970 and the Fair and Accurate Credit Transactions Act of 2003?
7. Describe a permissible purpose under the FCRA.
8. What is the purpose of a FCRA dispute letter?
9. What is a security or credit freeze?
10. What is the difference between the Safeguards Rule and the Red Flags Rule?

American online LIGS University

is currently enrolling in the
Interactive Online **BBA, MBA, MSc,**
DBA and PhD programs:

- ▶ enroll **by September 30th, 2014** and
- ▶ **save up to 16%** on the tuition!
- ▶ pay in 10 installments / 2 years
- ▶ Interactive **Online** education
- ▶ visit www.ligsuniversity.com to
find out more!

Note: LIGS University is not accredited by any
nationally recognized accrediting agency listed
by the US Secretary of Education.
More info [here](#).



4.9 ADDITIONAL LEARNING OPPORTUNITIES

1. The U.S. Department of Education has an excellent guide on FERPA that is available to parents. It is easy to read and includes a set of “Frequently Asked Questions” (FAQS). The Parents’ Guide to the *Family Educational Rights and Privacy Act: Rights Regarding Children’s Education Records* is available at <https://www2.ed.gov/policy/gen/guid/fpco/brochures/parents.html>.
2. The Federal Trade Commission has a consumer website that provides information on privacy, identity and online privacy. It also has a section on credit freeze “FAQS.” This information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

4.10 TEST YOUR LEARNING

- 1) A college in the western United States is seeking accreditation from a national agency. The accreditors request to review selected educational records. Do the accreditors have a legitimate educational interest to view the records?
 - a. No, only campus school officials have a legitimate educational interest.
 - b. No, only campus school officials and campus law enforcement have a legitimate educational interest.
 - c. No, only campus school officials, campus law enforcement and the disciplinary office have a legitimate educational interest.
 - d. Yes, as accreditors evaluating the educational process at the college, they have a legitimate educational interest to view the records.
- 2) Which of the following would be not considered directory information under FERPA?
 - a. Photograph
 - b. Date and place of birth
 - c. Parent’s name(s)
 - d. Telephone
 - e. Email address
- 3) FERPA violations are reported by
 - a. the filing of a civil complaints filed by the parent/guardian of a minor child.
 - b. the filing of a criminal complaints filed by the parent/guardian of a minor child or an aggrieved college student.
 - c. the filing of a civil complaint filed by the Department of Education.
 - d. discontinuance of federal funding.

- 4) What federal law protects a patient's medical records and health care information?
 - a. HIPAA
 - b. HIPPA
 - c. HITECH
 - d. ITECH
 - e. NVRAM

- 5) EHR stands for
 - a. electronic health care records
 - b. electronic hi-tech records
 - c. education and human resources
 - d. electronic human resources
 - e. events history recorder

- 6) Which of the following does not have a permissible purpose under FCRA to view a credit record?
 - a. bank
 - b. credit card company
 - c. insurance company
 - d. landlord
 - e. prospective employer

- 7) A key purpose of the Fair and Accurate Credit Transactions Act of 2003 is to
 - a. assist consumers repair their credit
 - b. assist consumers increase their credit limits
 - c. assist consumers placing a fraud alert on their credit file
 - d. assist consumers notifying credit agencies of a dispute

- 8) An extended fraud alert protects your credit for ____ years.
 - a. 2
 - b. 3
 - c. 5
 - d. 7
 - e. 10

- 9) The Privacy Rule refers to which law?
- a. The Financial Services Modernization Act of 1999
 - b. Safeguards Act
 - c. Meaningful Use of Health Information Technology Act
 - d. Non-public Personal Information Law
- 10) Which of the following voter information is private?
- a. your actual vote
 - b. your address
 - c. your political preferences
 - d. elections voted in
 - e. your Congressional District

Test Your Learning answers are located in the Appendix.

DON'T EAT YELLOW SNOW

What will your advice be?

Some advice just states the obvious. But to give the kind of advice that's going to make a real difference to your clients you've got to listen critically, dig beneath the surface, challenge assumptions and be credible and confident enough to make suggestions right from day one. At Grant Thornton you've got to be ready to kick start a career right at the heart of business.

Sound like you? Here's our advice: visit GrantThornton.ca/careers/students

Scan here to learn more about a career with Grant Thornton.

 **Grant Thornton**
An instinct for growth™

© Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd

5 PRIVACY AT WORK

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

- Describe the privacy rights of a job applicant during the pre-employment process;
- Explain the privacy rights and limitations an employee has in the workplace;
- Discuss the right of certain employers to require drug testing and yearly physicals of employees;
- Explain the requirements of the Employee Polygraph Protection Act, and how and when an employee must submit to a polygraph test;
- Describe the process an employer must follow to request an employee’s credit report;
- Explain what employees are covered under the Privacy Act of 1974;
- Describe GINA and why and how employers can be sued under this law; and
- Give an example of the importance of reviewing an employer’s BYOD policy.

5.1 OVERVIEW

Most legal scholars will agree that employees have little privacy at work. The basis for this statement is that the law recognizes an employer has the choice if, how and when it would like to monitor employee on the job activities. This includes **GPS tracking on company vehicles, computer and telephone monitoring**, as well as **video and audio surveillance** throughout the business. In other words, when an employee is being paid and using company equipment and resources, the law supports an employer’s monitoring of its employees.

As an employee, it is critical to be informed, and always review your company policy manual to understand your rights to *your* privacy.

Polygraph Tests	Drug Testing	Keylogging
Company Vehicles GPS	Employer Cell Phones GPS	Security Cameras
Monitoring of Internet Usage	Social Media	Phone Usage Review
Employee ID Tracking	Email Monitoring	Audio Recordings
Videotaping	Off Work Activities	Company Device Monitoring

Table 5-1: Examples of Employee Monitoring by Employees

5.2 THE PRE-EMPLOYMENT PROCESS

Privacy issues and concerns actually begin far before an employee is hired during the hiring and pre-employment investigation process. Certain actions are common practice and expected such as requiring documentation for earned degrees. But, can a prospective employer require the entire college or university transcript that details the grades the applicant received for each course? Can the prospective employer compel the candidate to complete a pre-employment physical, drug testing, as well as psychological testing? Can it demand the interviewee take a polygraph test? Lastly, it is legal for a potential employer to request a copy of a candidate's credit report as a condition of employment?

We consider each of these questions below. Note that the discussions for each of these questions, may have a different conclusion once a candidate is an employee of an organization. Additionally, state law implications may exist, but the responses below will focus on federal law.

5.2.1 TRANSCRIPT REQUESTS

Is it a violation of FERPA (*see* Chapter 4) for a prospective employer to require the entire college or university **transcript** that details the grades the applicant received for each course? FERPA is a federal law that limits *with whom the college or university* shares the information. A transcript belongs to the student, and the student controls who receives that information. So, if an employer requires the disclosure of that transcript as a condition for employment, it is the employer's right to require its submission as a condition of employment.

5.2.2 CREDIT REPORTS

Does the employer possess the ability to request an applicant's credit report? Clearly, this would be important information for an employer to know in the context of certain high security positions in government, banking, or finance. As earlier noted in Chapter 4, credit reports are covered under the FCRA. The FCRA contains specific language as to how an employer can receive a credit report, and the steps that must be taken if an applicant is rejected based on that report.

First, the employer must give notice to the candidate in writing and as a separate document that it may be using information from that report in making a hiring decision. Second, the employer must receive written authorization from the candidate to access the report. Third, the employer must provide written certification to the credit reporting agency they have complied with step one and step two. Fourth, if the employer makes a negative decision on the candidate based on the credit report, the company must provide the applicant with a copy of his or her credit report, a copy of the federal "**A Summary of Your Rights under the Fair Credit Reporting Act**,"²⁰¹ and written notification of the adverse action with specific information as detailed in Figure 5-1.

After You Take an Adverse Action

If you take an adverse action based on information in a consumer report, you must give the applicant or employee a notice of that fact – orally, in writing, or electronically.

An adverse action notice tells people about their rights to see information being reported about them and to correct inaccurate information. The notice must include:

- the name, address, and phone number of the consumer reporting company that supplied the report;
- a statement that the company that supplied the report did not make the decision to take the unfavorable action and can't give specific reasons for it; and
- a notice of the person's right to dispute the accuracy or completeness of any information the consumer reporting company furnished, and to get an additional free report from the company if the person asks for it within 60 days.

Figure 5-1: Materials in the public domain²⁰²

.....Alcatel-Lucent 

www.alcatel-lucent.com/careers

What if you could build your future and create the future?

One generation's transformation is the next's status quo. In the near future, people may soon think it's strange that devices ever had to be "plugged in." To obtain that status, there needs to be "The Shift".

5.2.3 PRE-EMPLOYMENT PHYSICALS AND DRUG TESTS

Can the prospective employer compel **pre-employment physicals, drug testing, and psychological evaluations**? The answer to this question also has compliance implications under the **American's with Disabilities Act of 1990**, 42 U.S.C. § 12101.²⁰³ The **ADA** applies to employers with over fifteen employees, and requires companies to provide a **“reasonable” accommodation** to its employees to enable completion of their jobs. A job applicant cannot be denied employment because the prospective employer does not want to provide an appropriate accommodation.²⁰⁴

THE LAW

The Americans with Disabilities Act of 1990 (ADA) prohibits discrimination and ensures equal opportunity for persons with disabilities in employment, State and local government services, public accommodations, commercial facilities, and transportation. It also mandates the establishment of TDD/telephone relay services. The ADA was revised by the ADA Amendments Act of 2008 (P.L. 110-325), which became effective on January 1, 2009. The ADA is codified at 42 U.S.C. 12101 et seq.

Figure 5-2: ADA Testing Restrictions of Employees – Materials in the public domain²⁰⁵

In general, this testing can be completed after 1) an offer has been made to a candidate (and it can be a conditional offer based on the results); 2) that all candidates are required to complete the testing; 3) that the testing is based on the ability to complete **“essential-job”** duties with or without a reasonable accommodation; and, 4) that the information from the testing is treated as a medical records subject to privacy requirements.

5.2.4 PRE-EMPLOYMENT POLYGRAPH TESTS

Can the prospective employer compel **pre-employment polygraph testing**? The federal **Employee Polygraph Protection Act (EPPA)**, 29 U.S.C. § 2001, restricts most pre-employment polygraph tests by commercial employers. However, the law excludes the federal, state, and local governments. Additionally, the law does not apply to those in the government, such as in the CIA or NSA, handling sensitive information. These types of entities often have other laws and regulations for pre-employment polygraph tests and under which circumstances polygraph tests can be administered.

The **U.S. Department of Labor** is the agency authorized with employer compliance with the EPPA. Again, private employers not covered by the EPPA cannot generally request a polygraph as a condition of employment.

Employee Polygraph Protection Act (EPPA)

Overview

The EPPA prohibits most private employers from using lie detector tests, either for pre-employment screening or during the course of employment. Employers generally may not require or request any employee or job applicant to take a lie detector test, or discharge, discipline, or discriminate against an employee or job applicant for refusing to take a test or for exercising other rights under the Act. Employers may not use or inquire about the results of a lie detector test or discharge or discriminate against an employee or job applicant on the basis of the results of a test, or for filing a complaint, or for participating in a proceeding under the Act. Subject to restrictions, the Act permits polygraph (a type of lie detector) tests to be administered to certain job applicants of security service firms (armored car, alarm, and guard) and of pharmaceutical manufacturers, distributors and dispensers.

Subject to restrictions, the Act also permits polygraph testing of certain employees of private firms who are reasonably suspected of involvement in a workplace incident (theft, embezzlement, etc.) that resulted in specific economic loss or injury to the employer. Where polygraph examinations are allowed, they are subject to strict standards for the conduct of the test, including the pretest, testing and post-testing phases. An examiner must be licensed and bonded or have professional liability coverage. The Act strictly limits the disclosure of information obtained during a polygraph test.

Figure 5-3: Department of Labor Overview of the EPPA – Materials in the public domain²⁰⁶

Additionally, the law requires employers to place a posting of Figure 5-4 (below) in the workplace to alert employees of their rights under this law.

EMPLOYEE RIGHTS

EMPLOYEE POLYGRAPH PROTECTION ACT

The Employee Polygraph Protection Act prohibits most private employers from using lie detector tests either for pre-employment screening or during the course of employment.

PROHIBITIONS	Employers are generally prohibited from requiring or requesting any employee or job applicant to take a lie detector test, and from discharging, disciplining, or discriminating against an employee or prospective employee for refusing to take a test or for exercising other rights under the Act.
EXEMPTIONS	<p>Federal, State and local governments are not affected by the law. Also, the law does not apply to tests given by the Federal Government to certain private individuals engaged in national security-related activities.</p> <p>The Act permits polygraph (a kind of lie detector) tests to be administered in the private sector, subject to restrictions, to certain prospective employees of security service firms (armored car, alarm, and guard), and of pharmaceutical manufacturers, distributors and dispensers.</p> <p>The Act also permits polygraph testing, subject to restrictions, of certain employees of private firms who are reasonably suspected of involvement in a workplace incident (theft, embezzlement, etc.) that resulted in economic loss to the employer.</p> <p>The law does not preempt any provision of any State or local law or any collective bargaining agreement which is more restrictive with respect to lie detector tests.</p>
EXAMINEE RIGHTS	Where polygraph tests are permitted, they are subject to numerous strict standards concerning the conduct and length of the test. Examinees have a number of specific rights, including the right to a written notice before testing, the right to refuse or discontinue a test, and the right not to have test results disclosed to unauthorized persons.
ENFORCEMENT	The Secretary of Labor may bring court actions to restrain violations and assess civil penalties against violators. Employees or job applicants may also bring their own court actions.

THE LAW REQUIRES EMPLOYERS TO DISPLAY THIS POSTER WHERE EMPLOYEES AND JOB APPLICANTS CAN READILY SEE IT.

WHD
WAGE AND HOUR DIVISION
UNITED STATES DEPARTMENT OF LABOR

1-866-487-9243
TTY: 1-877-889-5627
www.dol.gov/whd

WH 802 JUL 2016

Figure 5-4: EPPA Compliance Poster Required by the U.S. Department of Labor – Materials in the public domain²⁰⁷

5.3 THE EMPLOYEE-EMPLOYER RELATIONSHIP

After reading about the pre-interview process, the next question many ask is whether the privacy protections extended to job applicants, are also extended to those employed by a company. The answers to some questions are the same; and to others different.

Before reading further, readers should understand that as an employee, you should expect little privacy in the workplace, as discussed above. The law has supported the rights of employers to monitor activities on the job in a variety of ways. For example, video and audio surveillance are commonly found in the workplace (with the exceptions to physically invasive cameras being in personal places such as in a restroom, or locker room).



**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

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

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

www.mastersopenday.nl



Figure 5-5: Used with permission²⁰⁸

The lack of privacy at work also somewhat extends to an employee working at home. In other words, expect no privacy and limit your use of employer phones, computers, fax machines, etc. only to employer related tasks.

One key pivotal case that dealt with employee privacy was the case of *Michael A. Smyth v. The Pillsbury Company*, 914 F. Supp. 97 (E.D. Pa. 1996). This case involved an employee of Pillsbury Company by the name of Michael Smyth, who often worked from home. Smyth had been notified by his employer that the communications using the company email system were not private and could be reviewed by Pillsbury. Smyth, subsequently exchanged emails with a supervisor at Pillsbury, that the company deemed were “inappropriate and unprofessional.” Smyth’s employment was subsequently terminated by Pillsbury. The Court, in applying Pennsylvania law stated “we do not find that a reasonable person would consider the defendant’s interception of these communications to be a substantial and highly offensive invasion of his privacy. Again, we note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee’s person or personal effects. Moreover, the company’s interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.”²⁰⁹

This ruling is the position commonly and currently held by most U.S. Courts.²¹⁰

One Minute Challenge

Frankie works for the Lower Coalice Michigan School District. Frankie uses the School email system and address to send information to any attorney for a personal matter. Do you think that Frankie can and should be handling personal business matters through work email? The answer to the question is no. An employer owns the email system that Frankie is using, as well as the equipment. Unless the employer gives specific approval to employees to use company equipment and email systems for personal use, then Frankie may have potential issues with his employment with the School District. Always check your company's policies regarding the use of company email for personal use, as well as the repercussions for doing so.

5.3.1 CREDIT REPORT REVIEWS

The FCRA provides very similar privacy protections to both job applicants and employees. Written notification, consent and other requirements as described in Figure 5-1 also apply to current employees. In particular, FCRA applies to promotions, evaluations, and the discipline or termination of existing employees. Additionally, employers must comply with the law's "**disposal rule**," regarding consumer reports.²¹¹ This rule requires an employer to protect the privacy of the employee with the disposal of his or her *paper* personal information through appropriate means. Appropriate means not being simply placing records in the trash. Burning, pulverizing or the shredding of paper files meets the law's requirements. *Electronic information* must be destroyed appropriately "so that the information cannot be read or reconstructed."²¹² In addition, an appropriate disposal company should be contacted for appropriate destruction of the media.

5.3.2 MEDICAL TESTING

Medical (*i.e.*, physical) exams are generally limited to what is called "**fitness of duty**." Fitness of duty means that an employee has certain physical requirements in order to perform his or her job. This would apply, for example, to a law enforcement officer, or an airline pilot: professions in which physical health is a key element of successfully fulfilling the duties of the position. In occupations of this type, an employer can require a regular (typical yearly) physical examination. However, due to health care privacy laws, the employer does not receive details of the health exam, but rather only a result of whether the employee is fit to perform the duties required of the position. On the other hand, drug and alcohol testing on the job has different requirements. Federal law addresses this specifically with certain occupations such as airline pilots mentioned above, (which is regulated by the Federal Aviation Administration (FAA)). As an example, Figure 5-6 below provides a brief overview of mandatory drug and alcohol testing for aviation employees.

Industry Drug and Alcohol Testing Program

Are you keeping our skies safe?

Drug and alcohol testing of safety-sensitive aviation employees helps protect public safety and keep our skies safe. Testing is required by the Omnibus Transportation Employees Testing Act of 1991 and by DOT and FAA regulations (49 CFR part 40 and 14 CFR part 120).

The Drug Abatement Division oversees the aviation industry's compliance with the drug and alcohol testing law and regulations. We accomplish this by performing on-site inspections, providing guidance to companies, individuals, contractors, and service agents, and establishing policies and procedures to increase the program's effectiveness. We also develop and implement regulations for DOT/FAA drug and alcohol testing.

Figure 5-6: FAA Drug and Alcohol Testing for Aviation Employees – Materials in the public domain²¹³

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

Similarly, law enforcement officers have certain medical requirements. If you look for example at the requirements detailed by the Federal Bureau of Investigation in Figure 5-7 (below), you will see that alcohol, and both legal and illegal drug substances are discussed.

For the most part, employer drug testing requirements and limitations are based on state law. Federal laws will apply however to government employees and companies whose business is scrutinized by a federal agency, such as airlines by the Federal Aviation Administration.

EMPLOYMENT DRUG POLICY

The FBI is firmly committed to a drug-free society and workplace. Applicants for employment with the FBI who are currently using illegal drugs, misusing or abusing legal drugs or other substances at the time of the application process will be found unsuitable for employment. While the FBI does not condone any prior unlawful drug use by applicants, the FBI realizes some otherwise qualified applicants may have used illegal drugs at some point in their past. The guidelines set forth in this policy should be followed for determining whether an applicant's prior drug use makes him or her unsuitable for employment, balancing the needs of the FBI to maintain a drug-free workplace and the public integrity necessary to accomplish its law enforcement and intelligence missions by hiring the most qualified candidates to fill the FBI's personnel needs.

A candidate will be found unsuitable for employment and automatically disqualified if he/she deliberately misrepresents his or her drug history in connection with his or her application for employment. Additionally, candidates are automatically disqualified under the following criteria:

Marijuana Usage:

Candidates cannot have used marijuana within the three (3) years preceding the date of their application for employment, regardless of the location of use (even if marijuana usage is legal in the candidate's home state). The various forms of marijuana include cannabis, hashish, hash oil, and tetrahydrocannabinol (THC), in both synthetic and natural forms.

A candidate's use of marijuana in its various forms for medical reasons, regardless of whether or not it was prescribed by a licensed practicing physician, cannot be used as a mitigating factor.

Illegal Drugs:

Candidates cannot have used any illegal drug, other than marijuana, within the ten (10) years preceding the date of the application for employment.

Additionally, candidates cannot have sold, distributed, manufactured, or transported any illegal drug or controlled substance without legal authorization.

Prescription Drugs/Legally Obtainable Substances:

Candidates cannot have used anabolic steroids without a prescription from a licensed practicing physician within the past ten (10) years preceding the date of the application for employment.

Finally, candidates cannot have sold, distributed, manufactured, or transported any prescription drug without legal authorization.

Figure 5-7: Drug and Alcohol Testing Rules for Employees of the Federal Bureau of Investigation – Materials in the public domain²¹⁴

5.3.3 POLYGRAPH ADMINISTRATION

Polygraph testing of employees by private companies is illegal under **Employee Polygraph Protection Act** (EPPA). The key exception to this law would be security personnel or the investigation of an employment related crime. In the later scenario, the employee must be given at least 48 hours prior written notice that he or she is a suspect. Please refer back to Figure 5-4 (above), which includes a detailed review of employee rights regarding polygraph tests.

One Minute Challenge

Do you know the difference between a lie detector and a polygraph test? Under federal law (29 U.S.C. § 2001), a lie detector test is a polygraph. In fact under § 2001(3), the statute states that the word “‘lie detector’ includes a polygraph, deceptograph, voice stress analyzer, psychological stress evaluator, or any other similar device (whether mechanical or electrical) that is used, or the results of which are used, for the purpose of rendering a diagnostic opinion.”

5.3.4 PERSONNEL FILE REQUIREMENTS

Most employees don't think about privacy as to their personnel file, but the contents of that file are regulated by law and confidential. Federal employees are covered by the **Privacy Act of 1974**.²¹⁵ The Privacy Act of 1974 “establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.”²¹⁶

Information held on federal employees by a federal agency can be retrieved through a **Freedom of Information (FOIA)** request, which is a written request to an agency describing with particularity the information is being requested (*see* Chapter 6). FOIA requests are covered by the Freedom of Information Act.²¹⁷

The U.S. **Office of Personnel Management (OPM)** has determined that the following information can be given to the public through FOIA. As an example, the OPM has stated the following can information can be requested from an official military personnel file:

- Name
- Service Number
- Dates of Service
- Branch of Service
- Final Duty Status
- Final Rank
- Salary*
- Assignments and Geographical Locations
- Source of Commission*
- Military Education Level
- Promotion Sequence Number*

- Awards and decorations (eligibility only, not actual medals)
- Photograph
- Transcript of Courts-Martial Trials
- Place of entrance and separation
- (*indicates that information is rarely available in the records)²¹⁸

The distribution of information of non-federal employees are covered by individual state law. For example, Michigan provides the Bullard-Plawecki Employee Right to Know Act of 1978.²¹⁹ It allows an employee to make a written request to an employer for a personnel record, limiting the access to twice per year. The review should take place during normal business hours in a location close to the employer's place of business.

It is important that an employer does not commingle medical records in an employee's personnel file. They should be kept in a different file due to HIPAA (see Chapter 3) privacy rules. This would include documents such as work injuries, medical exam results, and documents relating to any request for accommodation.

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



5.4 GENETIC INFORMATION NONDISCRIMINATION ACT (GINA)

The **Genetic Information Nondiscrimination Act of 2008** limits the use of genetic information by employers to make hiring decisions and by insurance companies to determine the insurability of an applicant. As to employers, it is illegal:

- 1) to fail or refuse to hire, or to discharge, any employee, or otherwise to discriminate against any employee with respect to the compensation, terms, conditions, or privileges of employment of the employee, because of genetic information with respect to the employee; or
- 2) to limit, segregate, or classify the employees of the employer in any way that would deprive or tend to deprive any employee of employment opportunities or otherwise adversely affect the status of the employee as an employee, because of genetic information with respect to the employee.²²⁰

In addition to discrimination provisions, the law makes it unlawful for “an employer to request, require, or purchase genetic information with respect to an employee or a family member of the employee,” subject to certain conditions such as the consent of the employee,²²¹ or as part of an employee wellness program. The information cannot also be used against someone who is seeking health insurance, or as a way to set your premium.

Facts About the Genetic Information Nondiscrimination Act

Title II of the Genetic Information Nondiscrimination Act (GINA) protects individuals against employment discrimination on the basis of genetic information. GINA covers employers with 15 or more employees, including state and local governments. It also applies to employment agencies, labor organizations, joint labor-management training and apprenticeship programs, and the federal government.

Definition of Genetic Information

Genetic information means:

- Information about an individual's genetic tests;
- Information about the genetic test of a family member;
- Family medical history;
- Requests for and receipt of genetic services by an individual or a family member; and
- Genetic information about a fetus carried by an individual or family member or of an embryo legally held by an individual or family member using assisted reproductive technology.

Employment Decisions

GINA prohibits the use of genetic information in making employment decisions, such as hiring, firing, advancement, compensation, and other terms, conditions, and privileges of employment. For example, it would be illegal for an employer to reassign an employee from a job it believes is too stressful after learning of his family medical history of heart disease. There are no exceptions to the prohibition on using genetic information to make employment decisions.

Figure 5-8: Materials in the public domain²²²

The U.S. **Equal Employment Opportunity Commission (EEOC)** is responsible for compliance. The first lawsuit filed by the EEOC for GINA violations was against Fabricut, Inc., a distributors of decorative fabrics based in Tulsa, Oklahoma. The most recent lawsuit and settlement was against Joy Underground Mining who, after making a conditional employment offer, required a physical exam and family health history on a variety of ailments such as cancer, heart disease and diabetes. Below in Figure 5-9 is a copy of the press release from distributed by the EEOC regarding this case.

Joy Mining Machinery Settles EEOC Genetic Information Non-Discrimination Act Lawsuit

Mining Equipment Manufacturer Will Refrain From Requesting, Requiring or Purchasing Genetic Information

PITTSBURGH - Joy Underground Mining, LLC, trading as Joy Mining Machinery, will provide significant relief to settle a federal genetic information discrimination lawsuit filed by the U.S. Equal Employment Opportunity (EEOC), the agency announced today.

According to EEOC's lawsuit, after making conditional employment offers, Joy Mining required applicants to undergo a post-offer medical examination. EEOC charges that Joy Mining improperly requested family medical history on its pre-placement physical form asking applicants if they had a family medical history for "TB, Cancer, Diabetes, Epilepsy, [and] Heart Disease."

Such alleged conduct violates the Genetic Information Non-Discrimination Act (GINA), which protects individuals against employment discrimination on the basis of genetic information, including family medical history. GINA also prohibits employers from requesting, requiring or purchasing genetic information about applicants or employees, except in very narrow circumstances which do not apply in this case. EEOC filed suit (*EEOC v. Joy Underground Mining, LLC, t/a Joy Mining Machinery*, Civil Action No. 2:15-cv-01581-CRE) in U.S. District Court for the Western District of Pennsylvania after first attempting to reach a pre-litigation settlement through its conciliation process.

The two year consent decree resolving the lawsuit provides substantial equitable relief and prohibits Joy Mining Machinery from violating GINA and engaging in unlawful retaliation. Joy Mining Machinery will refrain from inquiring directly or indirectly about genetic information of an applicant, an applicant's family member, employee, or an employee's family member except as permitted by GINA. The company will also provide training on GINA to all management and human resources personnel with responsibilities related to hiring. The decree also provides for EEOC to monitor the company's compliance with decree provisions.

EEOC Philadelphia District Director Spencer H. Lewis, Jr. said, "Requiring an applicant or employee to answer questions about his or her family medical history, even when part of an otherwise permissible employment-related medical exam, violates federal law."

Regional Attorney Debra M. Lawrence of EEOC's Philadelphia District Office said, "We are pleased the Defendant cooperated with EEOC to reach an early resolution of this matter. This case illustrates the need for employers to review all employment-related procedures and forms after the passage of any new federal civil rights law regulating employment, such as GINA, to ensure prospective legal compliance."

EEOC's Philadelphia District Office has jurisdiction over Pennsylvania, Maryland, Delaware, West Virginia and parts of New Jersey and Ohio. The legal staff of EEOC's Philadelphia District Office also prosecutes discrimination cases arising from Washington, D.C. and parts of Virginia.

EEOC is responsible for enforcing federal laws against employment discrimination. Further information is available at www.eeoc.gov.

Figure 5-9: Materials in the public domain²²³

5.5 WORKING AT HOME AND BYOD (BRING YOUR OWN DEVICE)

When working at home and using your employer's equipment to complete work related tasks, the same rules apply, as previously discussed. Employers will be allowed to monitor those devices. However, what if you use your personal device for company tasks either in your home or in the office? The answer is unclear. However, the best option in answering the question is to refer to your company's policy on **BYOD** devices. For example, you might be using specialized software on your personal device and the **BYOD policy** might allow the employer to access the device, review your phone records and contacts, read your personal emails, and delete all data on the phone as company information could have been compromised. The policy might also allow the employer to view your browsing history, view text messages, access all photos, or even scrutinize your GPS location information. Remember that in the *City of Ontario v. Quon* (2010)²²⁴ case discussed in Chapter 1, the U.S. Supreme Court voted 9-0 to permit the search of a police officer's personal messages on a City owned pager. So, an employee should assume that any electronic device provided by an employer is monitored. Personal electronic equipment should not be used for business purposes, as the employer may have the legal right to search the device, and erase content as it deems appropriate.

An advertisement for SKF. The background is a blue-tinted image of a woman with long dark hair smiling, with a wind turbine visible behind her. The text is white and blue.

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

5.6 KEY TERMS

ADA American’s with Disabilities Act of 1990 Audio surveillance BYOD BYOD policy Computer monitoring Disposal rule EEOC Email monitoring Employee Polygraph Protection Act EPPA	Equal Employment Opportunity Commission Fitness of duty FOIA Freedom of Information Act GPS tracking on company vehicles Genetic Information Nondiscrimination Act of 2008 GINA Office of Personnel Management	OPM Pre-employment physical Pre-employment drug test Pre-employment psychological evaluation Privacy Act of 1974 Reasonable accommodation Summary of Your Rights under the Fair Credit Reporting Act Transcript requests U.S. Department of Labor Video surveillance
---	--	---

5.7 CHAPTER DISCUSSION QUESTIONS

1. What legal rights does a job applicant have regarding pre-employment health testing?
2. Are there certain situations where pre-employment health testing can be required?
3. Can an employer require to see a copy of your credit report as a condition of employment?
4. What is the ADA? What is a reasonable accommodation?
5. The Employee Polygraph Protection Act allows polygraph examinations of employees under what types of circumstances?
6. Why is the court ruling in the *Smyth* case significant?
7. What is fitness of duty? Who does it apply to?
8. What does the disposal rule require regarding the disposition of documents?
9. What is the Privacy Act of 1974?
10. Why was GINA enacted?

5.8 ADDITIONAL LEARNING OPPORTUNITIES

1. Learn more about the rules for fitness of duty physical examinations at <http://www.nolo.com/legal-encyclopedia/can-employer-require-me-to-take-fitness-duty-examination.html>.
2. For example, can a school district require an elementary special education teacher who has been hospitalized for AIDS to take a fitness of duty medical examination to return to his or her classroom duties?

5.9 TEST YOUR LEARNING

- 1) Which of the following is not a common type of employee monitoring?
 - a. GPS in company vehicles
 - b. GPS on personal phone
 - c. Audio monitoring in your office
 - d. Video monitoring in your office building
 - e. Email monitoring

- 2) The Genetic Information Nondiscrimination Act of 2008 applies to
 - a. private employers
 - b. public employers
 - c. insurance companies
 - d. a and b
 - e. all of the above

- 3) A prospective employer can access a copy of a college transcript if
 - a. it makes a verbal request to you and the college
 - b. it makes a written request to you and the college
 - c. it makes a request to you and you provide it to the employer
 - d. it is illegal for a prospective employer to request a college transcript

- 4) Employer access to credit reports is covered by
 - a. FCRA
 - b. FDIC
 - c. FERPA
 - d. FRCA
 - e. FOIA

- 5) Pre-employment physicals can be required of a candidate if
 - a. an offer has been made to a candidate.
 - b. an offer has been made to a candidate, and all candidates applying for the position are required to take physical.
 - c. an offer has been made to a candidate, all candidates applying for the position are required to take physical, and testing is based on the ability to complete essential job duties.
 - d. an offer has been made to a candidate, all candidates applying for the position are required to take physical, testing is based on the ability to complete essential job duties, and information from the tests are protected as confidential and private.

- e. an offer has been made to a candidate, all candidates applying for the position are required to take physical, testing is based on the ability to complete essential job duties, the information from the tests are protected as confidential and private, and the applicant does not need a work accommodation.
- 6) Fitness of duty means
- a. the employee exercises regularly
 - b. the employee has not been disciplined in the past three years
 - c. the employee meets the physical requirements of the job
 - d. the employee is a non-smoker
 - e. the employee does not use recreational marijuana
- 7) Polygraph testing
- a. is illegal for all employees
 - b. is illegal for some employees
 - c. is illegal for state employees
 - d. is illegal for federal employees
 - e. none of the above

TURN TO THE EXPERTS FOR **SUBSCRIPTION** CONSULTANCY

Subscribe is one of the leading companies in Europe when it comes to innovation and business development within subscription businesses.

We innovate new subscription business models or improve existing ones. We do business reviews of existing subscription businesses and we develop acquisition and retention strategies.

**Learn more at [linkedin.com/company/subscribe](https://www.linkedin.com/company/subscribe) or contact
Managing Director Morten Suhr Hansen at mha@subscribe.dk**

SUBSCR**IBE** - to the future

- 8) The Privacy Act of 1974 applies to
- state government agencies
 - federal government agencies
 - state and federal government agencies
 - private employers
 - foreign employers
- 9) What is a BYOD policy?
- a work policy on using personal devices for company tasks
 - a work policy on using personal devices for personal tasks
 - a work policy on using work devices for company tasks
 - a work policy on using work devices for personal tasks
- 10) What is the best statement about privacy at work?
- Do not expect privacy.
 - You have privacy on your personal phone.
 - You have privacy during your lunch hour.
 - You have privacy working at home.
 - You have privacy in a company car.

Test Your Learning answers are located in the Appendix.

6 PRIVACY AND GOVERNMENT

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

- Explain how information is collected through the Privacy Act of 1974 and what data is available for distribution to the public;
- Describe the exceptions to the distribution of information under the Privacy Act of 1974;
- Detail the provisions of Title III of the U.S.A. Patriot Act;
- State the changes made to the Electronic Communications Privacy Act by the U.S.A. Patriot Act;
- Summarize the changes made to the Foreign Intelligence Surveillance Act (FISA) by the U.S.A. Patriot Act;
- Compare the provisions of the U.S.A. Patriot Act to the U.S.A. Freedom Act; and
- Define the Freedom of Information Act and describe how to compose a FOIA letter.

6.1 OVERVIEW

Privacy and the government can be viewed from two opposing aspects: from the perspective of the federal government and from the perspective of the individual. Looking from the former, the federal government through its administrative authority collects and monitors information and data about individuals residing and visiting in the United States. This is done through a variety of laws such as the Privacy Act of 1974 (5 U.S.C. § 552a), The Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510 et seq.), and the U.S.A. Patriot Act.²²⁵

Looking from the latter, individuals want to understand how and under what circumstances people and organizations can request information from the federal government. Only information deemed to be of a “public” nature is open for review. Through the federal Freedom of Information Act (5 U.S.C. § 552), individuals and groups can secure copies of these communications.



Figure 6-1: Used with permission²²⁶

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

6.2 THE PRIVACY ACT OF 1974

According to the U.S. Department of Justice, the **Privacy Act of 1974**, “establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.”²²⁷ It should be emphasized that this law was enacted in 1974, during a time when the majority of records were maintained on paper. As retainment of records changed from paper to electronic, appropriate procedures were created to by federal agencies to comply with the law. Though, however, the U.S. Department of Justice has found fault with the current language of the law stating “the Act’s imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply.”²²⁸

One key aspect of this law is its applicability to U.S. citizens and permanent residents. Only those two groups of individuals have standing to sue under this law. Another interesting element of the law relates to Section 5 as written in 1974. This Section provided for the establishment of the **U.S. Privacy Protection Study Commission** to evaluate and make recommendations for changes to the law; however, the Commission was last operational in 1977, which at that time submitted a 690-page report to then President Jimmy Carter with its recommendations.²²⁹ In other words, it has been 40 years since the report was issued; however, privacy issues have dramatically changed over that period of time.

One significant Amendment to the Privacy Act did take place with the **Computer Matching and Privacy Protection Act of 1988** (5 U.S.C. § 552a). This law, effective December 31, 1989, “add(ed) procedural requirements for agencies to follow when engaging in computer-matching activities, provide matching subjects with opportunities to receive notice and to refute adverse information before having a benefit denied or terminated, and require that agencies engaged in matching activities establish Data Protection Boards to oversee those activities.”²³⁰ Amendments to Computer Matching and Privacy Protection Act were made in 1990 to clarify certain operational procedures.²³¹

Under the Privacy Act, the federal government cannot release information about an individual to a third party without that person’s consent. The law, however, provides 12 exceptions to the consent requirement. These include:

6.2.1 EXCEPTION 1.

5 U.S.C. § 552a(b)(1) (“need to know” within agency)

5 U.S.C. 552a(b)(1) states that information can be released without a person’s consent “to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.”²³² For example, an I.R.S. auditor in the performance of a taxpayer audit, may review a person’s prior tax returns without the taxpayer’s consent.

6.2.2 EXCEPTION 2.

5 U.S.C. § 552a(b)(2) (required FOIA disclosure)

The second exception is listed under 5 U.S.C. 552a(b)(2). This exception states as “required under section 552 of this title.” Section 552 is the federal Freedom of Information Act (FOIA). This means that information requested under FOIA, and meeting FOIA requirements, can be disclosed to a third party without the permission of the person who is the subject of the record.²³³

6.2.3 EXCEPTION 3.

5 U.S.C. § 552a(b)(3) (routine uses)

Section 552a(b)(3) of the Privacy Act is the third exemption. It provides for release of information if the use of the information is a “routine use” by a federal agency. This exemption is controversial,²³⁴ as the definition of routine is undefined by the law. However, this exemption was designed for the sharing of information between federal agencies.²³⁵ This exception would be useful for example, with the sharing of information between the Department of Homeland Security and other federal investigative agencies.

6.2.4 EXCEPTION 4.

5 U.S.C. § 552a(b)(4) (Bureau of the Census)

Exception 4 is detailed in Section 552a(b)4 and is known as the “census”²³⁶ exemption. This means that the U.S. Census Bureau can access your personal information “for purposes of planning or carrying out a census or survey or related activity.” Figure 6-2 provides information how you can locate information about yourself held by the U.S. Census Bureau.

Records About Yourself

The Privacy Act (PA) of 1974 is a Federal law that is set forth in Title 5, Section 552a, of the United States Code (5 U.S.C.552a), as amended. The purpose of the PA is to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and disclosure of personal information. In general, the PA allows individuals to learn how the Federal Government collects, maintains, uses, and disseminates records containing personal information. It also safeguards confidentiality by limiting or restricting disclosure of personally identifiable records maintained by Federal agencies. The PA allows individuals to gain access to their own personal records (unless the requested records are exempted from disclosure), and to seek correction or amendment of Federally maintained records that are inaccurate, incomplete, untimely, or irrelevant. As such, the PA establishes a "code of fair information practices," which requires Federal agencies to comply with statutory norms for collecting, maintaining, and disseminating records containing information about individuals

Under the Privacy Act, you may request copies of any Census Bureau records that:

- are about you, **and**
- are filed and can be retrieved by your name or by a personal identifier (such as your Social Security number).

You can also ask the Census Bureau to correct records that are inaccurate, incomplete, untimely, or irrelevant.

In some cases, the Privacy Act may not allow release of your personal records.

Figure 6-2: Sample Privacy Act Notice from the U.S. Census Bureau – Materials in the public domain²³⁷

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

6.2.5 EXCEPTION 5.

5 U.S.C. § 552a(b)(5) (statistical research)

The fifth exception under 5 U.S.C. Section 552a(b)5 allows disclosure “to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.”²³⁸ For example, assume the U.S. Department of Labor reports that in “manufacturing, productivity increased 1.0 percent and unit labor costs increased 2.2 percent.”²³⁹ The data gathering for the compilation of these statistics would be an exception under section 5.

6.2.6 EXCEPTION 6.

5 U.S.C. § 552a(b)(6) (National Archives)

Section 552a(b)(6) of Title 5, grants the National Archives and Administration (NARA) the authority to retrieve and compile “sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value.”²⁴⁰ For example, from the NARA website, one can request military service records on a family member. Additionally, many records are available online such as “Vietnam Conflict Records,” which includes casualty information, “Records of Medals, Awards and Decorations from the Vietnam Conflict,” as well as information and data on combat operations.²⁴¹

6.2.7 EXCEPTION 7.

5 U.S.C. § 552a(b)(7) (law enforcement request)

“This provision, in addition to providing for disclosures to federal law enforcement agencies, also allows an agency, ‘upon receipt of a written request, [to] disclose a record to another agency or unit of State or local government for a civil or criminal law enforcement activity.’”²⁴² For example, suppose the Ohio State Highway Patrol²⁴³ provides a written request to the Federal Bureau of Investigation for information regarding a convicted murderer who escaped from a Maryland state prison. This would be a valid request and an exception from the Privacy Act for criminal law enforcement purposes.

6.2.8 EXCEPTION 8.

5 U.S.C. § 552a(b)(8) (health or safety of an individual)

Assume the federal Occupational Safety and Health Administration, upon investigation of a manufacturing facility closes the plant as it has observed that several environmentally dangerous materials were found improperly stored on the plant property. Also assume there is evidence to suggest that former and current employees have been exposed to toxic chemicals from these products. The names of the former and current employees can be disclosed to the federal Center for Disease Control under Exception 8 to the Privacy Act. The scenario described suggests “compelling circumstances affecting the health or safety of an individual.”²⁴⁴

6.2.9 EXCEPTION 9.

5 U.S.C. § 552a(b)(9) (Congress)

Exception 9 allows members of Congress, as a participant in a Congressional Committee and a part of their Committee work, be allowed access to Privacy Act records.²⁴⁵

6.2.10 EXCEPTION 10.

5 U.S.C. § 552a(b) (10) (General Accounting Office)

Exception 10 gives the General Accounting Office (GAO),²⁴⁶ through the Comptroller General, or any authorized representative of the GAO to access to Privacy Act records.²⁴⁷

6.2.11 EXCEPTION 11.

5 U.S.C. § 552a(b) (11) (court order)

Exception 11 states Privacy Act records “may be disseminated pursuant to the order of a court of competent jurisdiction.”²⁴⁸ This means if a federal court in the District of Columbia orders the release of certain information covered under the Privacy Act, the information can be released without notice to the affected parties who are the subject of the records.

6.2.12 EXCEPTION 12.

5 U.S.C. § 552a(b) (12) (Debt Collection Act)

The last exception involves the federal Debt Collection Act. The law allows bad debt information to be shared with credit agencies, subject to a verification process that allows the debtor the opportunity to repay the debt prior to release of the information.²⁴⁹

6.2.13 EXEMPTIONS

There are also 10 exemptions under the Privacy Act.²⁵⁰ The difference between an exception and an exemption is that an exemption specifically disallows release of certain records. In other words, lawmakers made an intentional choice that the law not cover the circumstances described in an exemption. An exception on the other hand, is a situation included in the law, that may have different requirements to be covered.

A. One Special Exemption -- 5 U.S.C. § 552a(d)(5)

“nothing in this [Act] shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.”

Figure 6-3: Materials in the public domain²⁵¹

6.2.14 DAMAGES

Individuals may sue for violations of the Privacy Act and receive actual damages. The U.S. Supreme Court has determined the phrase “actual damages” does not include damages for mental or emotional distress, as they are not specifically authorized by the law.²⁵²

This e-book
is made with
SetaPDF



SETASIGN



PDF components for PHP developers

www.setasign.com

6.3 U.S.A. PATRIOT ACT

The full title of the law is “**The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.**” This law was signed in response to the attacks on the United States on September 11, 2001. The **Patriot Act** was passed quickly and signed into law by then President George Bush on October 25, 2001. It became effective October 26 of that year. The law had very strong bi-partisan support with a vote of Senate 98-1, and 357-66 in the House. The intent of the law was to grant law enforcement the authority to eavesdrop, use surveillance, and monitor the activities of suspected terrorists. It also facilitated information sharing between government agencies, and increased the penalties for those committing terrorist crimes.

The original version of the Patriot Act consisted of ten sections or Titles. Key provisions of the law are included in Title III. A listing of the Titles and subsections are detailed in Table 6.1 below.

Title I	ENHANCING DOMESTIC SECURITY AGAINST TERRORISM
Title II	ENHANCED SURVEILLANCE PROCEDURES
Title III	INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001
Subtitle A	International Counter Money Laundering and Related Measures
Subtitle B	Bank Secrecy Act Amendments and Related Improvements
Subtitle C	Currency Crimes and Protection
Title IV	PROTECTING THE BORDER
Subtitle A	Protecting the Northern Border
Subtitle B	Enhanced Immigration Provisions
Subtitle C	Preservation of Immigration Benefits for Victims of Terrorism
Title V	REMOVING OBSTACLES TO INVESTIGATING TERRORISM
Title VI	PROVIDING FOR VICTIMS OF TERRORISM, PUBLIC SAFETY OFFICERS, AND THEIR FAMILIES
Subtitle A	Aid to Families of Public Safety Officers
Subtitle B	Amendments to the Victims of Crime Act of 1984

Title VII	INCREASED INFORMATION SHARING FOR CRITICAL INFRASTRUCTURE PROTECTION
Title VIII	STRENGTHENING THE CRIMINAL LAWS AGAINST TERRORISM
Title IX	IMPROVED INTELLIGENCE
Title X	MISCELLANEOUS

Table 6-1: Titles and Subtitles of the U.S.A. Patriot Act²⁵³

In addition, the Patriot Act amended several other laws as noted in Table 6.2 below. Of significance were changes the law made to the **Electronic Communications Privacy Act (ECPA)**, and the **Foreign Intelligence Surveillance Act (FISA)**, which will be discussed in more detail in this chapter.

<p>U.S.A. Patriot Act</p> <p>The original law is broken down into several different provisions (or ten Titles). It also created amendments to existing law. These amended laws include the:</p> <ul style="list-style-type: none"> • Bank Secrecy Act; • Computer Fraud and Abuse Act; • Electronic Communications Privacy Act; • Fair Credit Reporting Act; • Family Education Rights and Privacy Act; • Foreign Intelligence Surveillance Act; • Immigration and Nationality Act; • Money Laundering Act; • Money Laundering Control Act; • Pen Register and Trap and Trace Statute; and • Right to Financial Privacy Act.
--

Table 6-2: Laws Effected by the U.S.A. Patriot Act²⁵⁴

6.3.1 TITLE III

Title III²⁵⁵ is a stand-alone law called the **International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001** (31 U.S.C. § 5301). The key purpose of the law was to place controls in the U.S. monetary and banking systems to stop terrorists from financing operations through money laundering inside of and outside of the United States.

There are three sections to Title III. Subtitle A is referred to as the section on **International Counter Money Laundering and Related Measures**. Subtitle B is the **Bank Secrecy Act Amendments and Related Improvements**. Subtitle C deals with **Currency Crimes and Protection**.

6.3.1.1 SUBTITLE A. INTERNATIONAL COUNTER MONEY LAUNDERING AND RELATED MEASURES

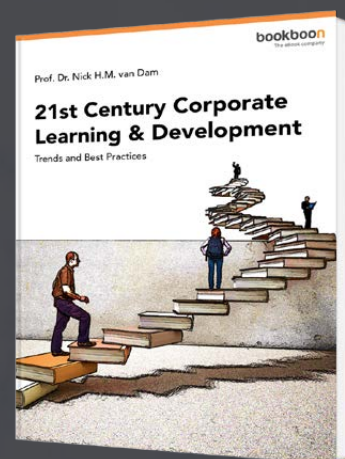
This section of the Patriot Act places requirements on U.S. banking institutions to maintain strict and detailed records on financial transactions *that involve international institutions*. Required information can include the names and addresses of those involved in the transaction (both sending and receiving), and a description of the transaction.

The term “**beneficial owner**” is often referenced in Subtitle A. In this context, beneficial owner refers to the person(s) receiving the funds, who is/are not the person(s) making the original transfer. The law assumes that terrorist funded transactions may come from sources not directly connected with the actual recipient of the funds.

Free eBook on Learning & Development

By the Chief Learning Officer of McKinsey

Download Now



6.3.1.2 SUBTITLE B – BANK SECRECY ACT AMENDMENTS AND RELATED IMPROVEMENTS

Subtitle B deals with U.S. financial transactions and places restrictions *on cash transactions in the U.S.* to minimize money laundering and the funding of illegal activities including terrorist financing.

Money laundering is the process of taking money procured through an illegal means and to “funnel” that money through a legal source to legitimize the funds. For example, suppose an illegal drug operation wants to legitimize \$10,000 in drug profits. To do this the funds are given to a local construction company who deposits the cash in a bank by making several small deposits. (Note that under federal law, any cash deposit over \$10,000 or any suspicious cash transaction such as making several small cash deposits at one time, must be reported by the bank to the Internal Revenue Service.)²⁵⁶

Money Laundering and Terrorist Financing

The central purpose of the Bank Secrecy Act is to help identify situations when the U.S. financial system and the institutions that comprise that system may be used to facilitate money laundering, terrorist financing and other illicit financing activities. In both money laundering and terrorist financing, criminals are able to exploit the openness of our financial system to launder criminal proceeds, or to support terrorist activity, and ultimately, to hide their true purpose.

Money laundering is the criminal practice of filtering ill-gotten gains or "dirty" money through a maze or series of transactions, so the funds are "cleaned" to look like proceeds from legal activities. Although money laundering can be diverse and complex, it basically involves three independent steps that can occur simultaneously: the "placement" of the unlawful proceeds into the financial system in an effort to avoid attracting the attention of law enforcement; the "layering" of the proceeds through a series of transactions to create confusion about the origin and true owner of the funds, and complicate the paper trail; and the "integration" of the proceeds wherein the launderers seek to create the appearance of legitimacy through additional transactions.

In contrast with money laundering, the motivation behind terrorist financing is ideological rather than profit-based. Typically, terrorist financing includes the use of both clandestine and legitimate sources of financing, which is a key difference from traditional money laundering. However, terrorists and their support organizations have been found to use the same methods as other criminal groups to launder funds. For example, law enforcement reports that terrorist financiers use currency smuggling; structured deposits to, or withdrawals from, bank accounts; purchases of various types of monetary instruments; and circuitous funds transfers in order to hide financial support. Terrorist financing is generally more difficult for banking organizations to identify. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex. The movement of small sums of money for laundering or terrorist purposes can be a challenge for a banking organization to identify with no other information.

Figure 6-4: Materials in the public domain²⁵⁷

6.3.1.3 Subtitle C – Currency Crimes and Protection

This section of the law details the elements of currency crimes and the punishments involved with violations of those crimes. It deals with the counterfeiting of U.S. currency, and the bulk smuggling of money. **Bulk smuggling** is the movement of large amounts of cash (over \$10,000) or monetary instruments to or from U.S. borders, to evade currency reporting requirements.²⁵⁸ It is regularly used by illegal enterprises (such as drug traffickers). Specifically, the law states:

Whoever, with the intent to evade a currency reporting requirement, knowingly conceals more than \$10,000 in currency or other monetary instruments on the person of such individual or in any conveyance, article of luggage, merchandise, or other container, and transports or transfers or attempts to transport or transfer such currency or monetary instruments from a place within the United States to a place outside of the United States, or from a place outside the United States to a place within the United States, shall be guilty of a currency smuggling offense (31 U.S.C § 5332).²⁵⁹

Penalties for violation of the law include the forfeiture of the funds being smuggled, and up to five years in prison.



Figure 6-5: Example of a forfeiture by the U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) – Materials in the public domain²⁶⁰

6.3.2 THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) OF 1986

The ECPA was passed to create “fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.”²⁶¹ Specifically, it “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.”²⁶²

The law consists of three Titles: Title I include amendments to the **Wiretap Act** (often referred to as the **Electronic Privacy Act**), Title II created the **Stored Communications Act**, and Title III created the **Pen Register Act**. The ECPA was significantly amended by the **Communications Assistance to Law Enforcement Act (CALEA)** in 1994, the **USA PATRIOT Act** in 2001, the **USA PATRIOT Reauthorization Act in 2006**, and the **FISA Amendments Act of 2008**.²⁶³



www.sylvania.com

We do not reinvent
the wheel we reinvent
light.

Fascinating lighting offers an infinite spectrum of possibilities: Innovative technologies and new markets provide both opportunities and challenges. An environment in which your expertise is in high demand. Enjoy the supportive working atmosphere within our global group and benefit from international career paths. Implement sustainable ideas in close cooperation with other specialists and contribute to influencing our future. Come and join us in reinventing light every day.

Light is OSRAM

OSRAM
SYLVANIA



6.3.2.1 TITLE I: WIRETAP ACT (ELECTRONIC PRIVACY ACT)²⁶⁴

“Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or ‘procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.’”²⁶⁵ For example, assume that a law enforcement officer fails to procure a proper search warrant for a wiretap, or has a court order for a wiretap, but monitors communications not specifically detailed in the wiretap order. In this situation, both of these communications would have been obtained illegally, and they could not be used as evidence in a criminal prosecution.²⁶⁶

6.3.2.2 TITLE II: STORED COMMUNICATIONS ACT²⁶⁷

The second Title of the ECPA is known more commonly as the Stored Communications Act or the SCA. This statute is a privacy law that requires Internet Service Providers (ISPs) and other companies who store computer communications (all types including verbal, wire and electronic) to keep private information such a customer’s name and their billing and service records.²⁶⁸

6.3.2.3 TITLE III: PEN REGISTER ACT

The Pen Register Act²⁶⁹ is also known as Title III of the ECPA. It regulates the use of pen register and trap and trace devices. A pen register is “a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject”.²⁷⁰ A trap and trace is “a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated.”²⁷¹

Actual calls are not captured and recorded under the Pen Register Act. Instead metadata (non-content data) is captured, such as phone numbers, date of the call, source of the call, and the recipient of the call.

This information can be acquired by federal law enforcement agencies through an “**authorization order.**” According to the U.S. Department of Justice, an authorization order “can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applicant’s agency.”²⁷²

6.3.2 THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

FISA²⁷³ was originally passed in 1978 to allow secret federal surveillance activities to protect the national security of the United States. As written, the law also created a secret **Foreign Intelligence Surveillance Court**,²⁷⁴ which rules on requests by the U.S. government for “electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes.”²⁷⁵ A second court, the **Foreign Intelligence Surveillance Court of Review (FISCR)** hears appeals from the Foreign Intelligence Surveillance Court. The Court of Review, also established in 1978 is composed of three judges either from the U.S. District Court or U.S. Court of Appeals. The Chief Justice of the U.S. Supreme Court determines the judges appointed to the Court of Review.²⁷⁶

About the Foreign Intelligence Surveillance Court

The Foreign Intelligence Surveillance Court was established in 1978 when Congress enacted the Foreign Intelligence Surveillance Act (FISA), which is codified, as amended, at 50 U.S.C. §§ 1801-1885c. The Court sits in Washington D.C., and is composed of eleven federal district court judges who are designated by the Chief Justice of the United States. Each judge serves for a maximum of seven years and their terms are staggered to ensure continuity on the Court. By statute, the judges must be drawn from at least seven of the United States judicial circuits, and three of the judges must reside within 20 miles of the District of Columbia. Judges typically sit for one week at a time, on a rotating basis.

Pursuant to FISA, the Court entertains applications submitted by the United States Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. Most of the Court's work is conducted ex parte as required by statute, and due to the need to protect classified national security information.

- Additional information concerning the operation of the Court can be found at:
[Letter to Chairman Leahy, Committee on the Judiciary, United States Senate July 29, 2013](#)
- The Judges who have served on the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review can be found at:
[FISC FISCR JUDGES May 20 2016](#)

Figure 6-6: Materials in the public domain²⁷⁷

As noted, the Patriot Act made amendments to FISA. Key changes included those to **Section 206** of the Patriot Act that allowed for roving wiretaps and the ability of law enforcement to follow a targeted subject to various locations. **Section 207** was also changed to allow the government “to conduct electronic surveillance and physical search of certain agents of foreign powers and nonresident alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year.”²⁷⁸ Additionally, **Section 215** was modified and expanded the materials that could be requested by a federal law enforcement agency to include “any tangible thing,” such as business records that might relate to national security.

In 2004 another modification to the law was made. It involved Section 6001(a) of the **Intelligence Reform and Terrorism Prevention Act (IRTPA)**²⁷⁹ (also known as the “**lone wolf**” provision) giving power to the U.S. government to monitor the activities of “non-U.S. persons” believed to be involved in international terrorist actions, without having *specific known ties* to a terrorist organization.

In 2011, President Obama signed into law the **Patriot Sunsets Extension Act of 2011**²⁸⁰ reauthorizing the three key provisions of the Patriot Act (§ 206 dealing with roving wiretaps, the § 215 expansion of tangible records to include business records, and the lone wolf provision of IRTPA), but the law also included a four-year sunset expiration provision.

In June of 2015, after much controversy, key elements of the Patriot Act were again renewed by the **USA Freedom Act**.²⁸¹ Section 206 on roving wiretaps was reapproved as was the lone wolf provision of the IRTPA. However, due to privacy concerns, Section 215 was modified to prohibit the bulk collection of all telephone records and the limit collection of call logs by the National Security Agency to *only* those identified as targets for surveillance, or who posed a potential or real threat to national security. Additionally, the FISA pen register authority was eliminated. Lastly, the FISA Court was ordered to declassify “(a)ll significant constructions or interpretations of law” by it in its rulings. FISA Court rulings can be reviewed at its website.²⁸²

6.4 TRAVELER SURVEILLANCE AND SCREENING

After the 9-11 terrorist attacks on the United States, many travel restrictions and policies were enacted. Two major changes involved traveler surveillance and the process for the screening of passengers.



Discover the truth at www.deloitte.ca/careers

Deloitte.

© Deloitte & Touche LLP and affiliated entities.

Regarding these changes, the **Transportation Security Administration (TSA)**, an arm of the Department of Homeland Security is responsible for 1) screening those who fly, and 2) the surveillance and safety of air travel.

The TSA states it uses a “**risk-based, intelligence-driven strategy**”²⁸³ for the screening of passengers. Its first line passenger security program is called “**Secure Flight**” that prescreens passengers identifying them as low or high risk. This is done by reviewing passenger lists against watch lists, and those not allowed to fly for security reasons. Minimal personal information is used in this process as noted below in the TSA’s privacy policy shown in Figure 6-7.

To protect privacy, the Secure Flight program collects the minimum amount of personal information, such as full name, date of birth, and gender, necessary to conduct effective matching. Read the [Privacy Impact Assessment](#) and the [System of Records Notice](#) for information about the program's rigorous privacy protections. Personal data is collected, used, distributed, stored and disposed of according to stringent guidelines.

Secure Flight transmits the screening instructions back to the airlines to identify low-risk passengers eligible for TSA Pre✓*; individuals on the Selectee List who are designated for enhanced screening; and those who will receive standard screening. Secure Flight also prevents individuals on the No Fly List and Centers for Disease Control and Prevention Do Not Board List from boarding an aircraft. The [Travel Redress Program](#) provides resolution for travel-related screening or inspection issues.

Figure 6-7: Materials in the public domain²⁸⁴

Privacy advocates have often questioned the privacy and appropriateness of the screening technology used by the TSA, which includes both “**millimeter wave advanced imaging technology** and **walk-through metal detectors**.”²⁸⁵ The TSA states that this technology does not take “**passenger-specific images**.” Rather it uses a “**generic outline**” of a person that is programmed with specific threat areas used to conceal objects such as explosives.²⁸⁶

In addition, the U.S. Drug Enforcement Administration (DEA) regularly monitors traveler information and profiles individuals believed to be involved in drug trafficking. Information gained from the profiling can be used for arrests and cash seizures.²⁸⁷

6.5 WIKILEAKS

The name “**WikiLeaks**” often is associated with the breach of information obtained through illegal means such as hacking. WikiLeaks²⁸⁸ is an organization created by an Australian, Julian Paul Assange. The groups states that it “specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption.”²⁸⁹ It self-reports “it has so far published more than 10 million documents and associated analyses.”²⁹⁰

How does WikiLeaks work? Information obtained by anonymous hackers is posted on its website and or shared with news alliances throughout the world. This leaked information may include documents relating to the national security of a country, or in the case of the 2016 U.S. Presidential elections, the leaking of emails from the Democratic National Committee and its campaign.²⁹¹

In the United States, WikiLeaks first major publicized event involved **Sgt. Chelsea (Bradley) Manning**,²⁹² who was accused, court martialled and found guilty of violations of the U.S Espionage Act for sharing thousands of documents to WikiLeaks.

No major country has been immune from a WikiLeaks posting. A review of its website includes documents released from Saudi Arabia, Germany, Australia, and Syria.²⁹³

6.6 EDWARD J. SNOWDEN

In 2013, a former CIA employee and contractor at the National Security Agency by the name of **Edward J. Snowden**, created international headlines upon revealing to the world details of secret surveillance programs being operated by the NSA and other European security agencies across the world. Feeling his actions were moral, but knowing they were illegal, Snowden left his job in Hawaii, and traveled to Hong Kong where he released details of classified information to reporters from the *London Guardian* and the *New York Times*. Snowden subsequently moved to the Soviet Union, where he currently has asylum. He is unapologetic for the disclosure, as he states the materials were released so the American public would know about the illegal mass surveillance of emails, phone calls, contact lists, text messages and cell phone location tracking, which he felt to be unconstitutional and a privacy violation never authorized by the U.S. Congress. The exact number of documents taken by Snowden is unknown, but some experts estimate it to be in the range of 1.7 million.²⁹⁴

Snowden has been characterized as a traitor by some, and a hero by others. However, he has been charged by the U.S. Department of Justice with **theft of government property** (18 U.S.S. § 641), the **unauthorized communication of national defense information** (18 U.S.C. § 793(d)), and **the willful communication of classified communications intelligence information to an unauthorized person** (18. U.S.C. § 98(a)(3)) as described in Figure 6-8 below. The latter two offenses are often referred to as espionage crimes.²⁹⁵

6.7 PUBLIC INFORMATION AND THE FREEDOM OF INFORMATION ACT

Public information is data legally collected by the government, that may or may not be readily available to the public.

The release of public information is governed by both state and federal law. Most information is possessed at a state or local level. However, federal court records, military information, federal offender records, naturalization records and Social Security records may be located online.

For information not readily available on the Internet, both the individual states and the federal government are subject to **Freedom of Information Act (FOIA)** laws. FOIA laws, as they are most commonly called, are meant to allow members of the public to retrieve and access records held by government entities, subject to certain restrictions. The Federal FOIA Act was created in 1967.

What is FOIA?

The Freedom of Information Act (FOIA) is a law that gives you the right to access information from the federal government. It is often described as the law that keeps citizens in the know about their government.

Figure 6-9: Materials in the public domain²⁹⁷

So, how does FOIA work? Federal law is very clear on the process. First, the records sought from the federal agency must be determined. Specificity is important because a request may be denied if it is too broadly worded. Second, a written request must be filed with the federal agency requesting the information under the FOIA Act. Electronic requests are accepted by federal agencies. Note that the federal agency may charge for copy costs, so a request should include the dollar amount for copies; however, “there is usually no charge for the first two hours of search time or for the first 100 pages of duplication.”²⁹⁸

Certain information is exempt under the law from FOIA requests. These include:

Exemption 1: Information that is classified to protect national security.

Exemption 2: Information related solely to the internal personnel rules and practices of an agency.

Exemption 3: Information that is prohibited from disclosure by another federal law.

Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged.

Exemption 5: Privileged communications within or between agencies, including:

1. Deliberative Process Privilege
2. Attorney-Work Product Privilege
3. Attorney-Client Privilege

Exemption 6: Information that, if disclosed, would invade another individual's personal privacy.

Exemption 7: Information compiled for law enforcement purposes that:

- 7(A). Could reasonably be expected to interfere with enforcement proceedings
- 7(B). Would deprive a person of a right to a fair trial or an impartial adjudication
- 7(C). Could reasonably be expected to constitute an unwarranted invasion of personal privacy
- 7(D). Could reasonably be expected to disclose the identity of a confidential source
- 7(E). Would disclose techniques and procedures for law enforcement investigations or prosecutions
- 7(F). Could reasonably be expected to endanger the life or physical safety of any individual

Exemption 8: Information that concerns the supervision of financial institutions.

Exemption 9: Geological information on wells.²⁹⁹

Federal FOIA law also excludes certain information from the law. These include ongoing federal criminal investigations, information regarding informants, and classified "foreign intelligence or counterintelligence, or international terrorism records."³⁰⁰

Sample FOIA Request Letter³⁰¹

Date _____

Agency FOIA Officer
 Name of agency or agency component
 Address (see who to contact ³⁰²)

Dear _____

Under the Freedom of Information Act, 5 U.S.C. subsection 552, I am requesting access to [identify the records as clearly and specifically as possible].

If there any are feeds for copying the records, please let me know before you work on my request. [Or, please supply the records without informing me of the cost if the fees do not exceed \$ _____ which I agree to pay.]

If you deny all or any part of this request, please cite each specific exemption you think justifies your refusal to release the information and notify me of appeal procedures available under the law.

Optional: If you have any questions about handling this request, you may telephone me at _____ (home phone) or at _____ (office phone).

Sincerely,

Name _____
 Address _____

Figure 6-10: Materials in the public domain³⁰³





- The number 1 MOOC for Primary Education
- Free Digital Learning for Children 5-12
- 15 Million Children Reached

About e-Learning for Kids Established in 2004, e-Learning for Kids is a global nonprofit foundation dedicated to fun and free learning on the Internet for children ages 5 - 12 with courses in math, science, language arts, computers, health and environmental skills. Since 2005, more than 15 million children in over 190 countries have benefitted from eLessons provided by EFK! An all-volunteer staff consists of education and e-learning experts and business professionals from around the world committed to making difference. eLearning for Kids is actively seeking funding, volunteers, sponsors and courseware developers; get involved! For more information, please visit www.e-learningforkids.org.

6.8 KEY TERMS

<p>Authorization order Bank Secrecy Act Amendments and Related Improvements Beneficial owner Bulk Smuggling Communications Assistance to Law Enforcement (CALEA) Computer Matching and Privacy Protection Act of 1988 Currency Crimes and Protections Edward J. Snowden Electronic Communications Privacy Act (ECPA) FISA Amendments Act of 2008 Foreign Intelligence Surveillance Court Foreign Intelligence Surveillance Court of Review (FISCR)</p>	<p>Foreign Intelligence Surveillance Act (FISA) Generic outline Intelligence Reform and Terrorism Prevention Act (IRTPA) International Counter Money Laundering and Related Measures International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 Lone wolf Millimeter wave advanced imaging technology Passenger specific images Patriot Sunsets Extension Act of 2011 Pen Register Act Privacy Act of 1974 Risk-based, intelligence driven strategy Secure Flight Section 206</p>	<p>Section 207 Section 215 Sgt. Bradley (Chelsea) Manning Stored Communications Act Theft of government property Title III Transportation Security Administration (TSA) Unauthorized communication of national defense information U.S. Privacy Protection Study Commission U.S.A. Patriot Act U.S.A. Patriot Reauthorization Act of 2006 Walk through metal detectors Wikileaks Willful communication of classified communications intelligence information to an unauthorized person Wiretap Act</p>
--	---	--

6.9 CHAPTER DISCUSSION QUESTIONS

1. What is the purpose of the Privacy Act of 1974?
2. Based on the date of the Privacy Act, is it still a current and useful law?
3. What was the purpose of the U.S.A. Patriot Act?
4. What is the most significant section of the U.S.A. Patriot Act? Why?
5. What is a beneficial owner? What law refers to this term?
6. What is bulk smuggling? In what law is it used? What are the penalties for bulk smuggling?
7. What is the difference between the Wiretap Act and Stored Communications Act?
8. How does the Pen Register Act operate?
9. Describe three situations in which a person would use the Freedom of Information Act to access information?
10. Who is Edward J. Snowden? Why has he been charged with the violation of three federal crimes?

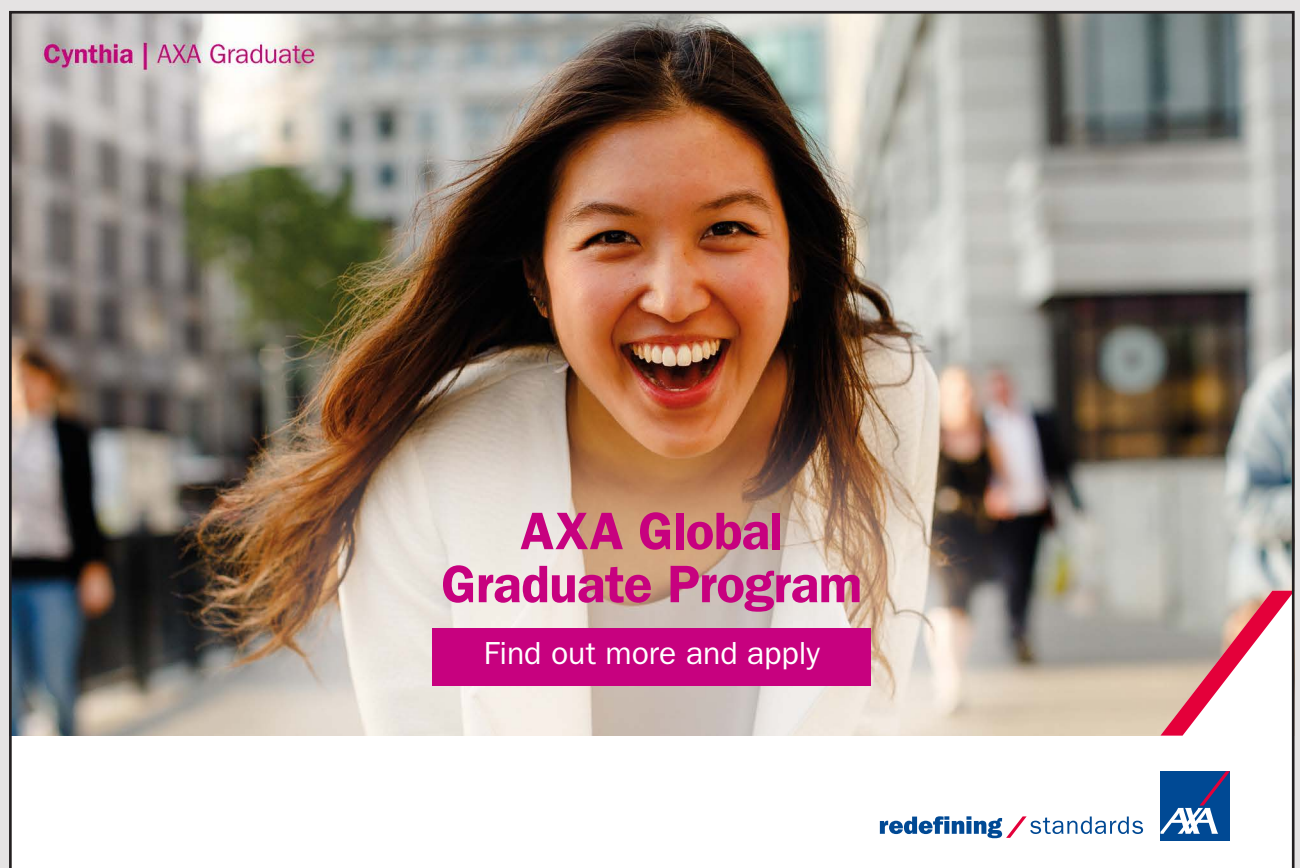
6.10 ADDITIONAL LEARNING OPPORTUNITIES

1. The Electronic Frontier Foundation has a section on its website that provides information on the law of government surveillance. Check out their Surveillance Self Defense project at <https://ssd.eff.org/>.
2. The Electronic Frontier Foundation has an excellent section on privacy. It discusses the legal and practical issues of privacy including anonymity, biometrics, border searches, cell tracking, encrypting the web, international privacy standards, locational privacy, mass surveillance technologies, medical privacy, national security letters, NSA spying, PATRIOT Act, pen traps, student privacy, surveillance drones, and travel screening. The information can be located at <https://www.eff.org/issues/privacy>.

6.11 TEST YOUR LEARNING

1. What is a pen register?
 - a. It is a device that records landline telephone calls.
 - b. It is a device that records cell phone calls.
 - c. It is a device that captures text messages.
 - d. It is a device that captures non-content data from phone calls.
2. The Electronic Communications Privacy Act consists of how many titles?
 - a. 1
 - b. 2
 - c. 3
 - d. 4
 - e. 5
3. The Pen Register Act is also known as Title III of the
 - a. ECPA
 - b. U.S.A. Patriot Act
 - c. CALEA
 - d. FISA Act
 - e. FOIA
4. What is the purpose of the Foreign Intelligence Surveillance Court?
 - a. To rule on applications for physical searches for foreign intelligence purposes.
 - b. To rule on applications for electronic surveillance for foreign intelligence purposes.
 - c. To rule on applications for investigative actions for foreign intelligence purposes.
 - d. To rule on applications to search for business records for foreign intelligence purposes.
 - e. All of the above


5. Which section of the U.S.A. Patriot Act allows roving wiretaps?
- 203
 - 206
 - 207
 - 209
 - The U.S.A. Patriot Act does now allow for roving wiretaps. The IRTPA does.
6. What law includes a lone wolf provision?
- Foreign Intelligence Surveillance Act
 - Intelligence Reform and Terrorism Prevention Act
 - Patriot Sunsets Extension Act of 2011
 - U.S.A. Freedom Act
 - U.S.A. Patriot Act
7. Jesse makes a request for classified information under a FOIA request. The request
- will not be granted, as the information is classified to protect national security.
 - will not be granted, as the information is a trade secret and confidential.
 - will not be granted, as the information, if disclosed would invade another person's personal privacy.
 - will be granted as it is a reasonable request under federal FOIA laws.



Cynthia | AXA Graduate

AXA Global Graduate Program

Find out more and apply

redefining / standards 

8. Under the Privacy Act of 1974, the law provides information can be released with a person's consent if
 - a. it is one of the 12 exceptions allowed under the law.
 - b. a FISA Court orders it released.
 - c. it is census information.
 - d. Consent is always required.

9. Money laundering means to
 - a. take money derived from an illegal activity and legitimize the funds through a legal alternative.
 - b. literally wash money to remove any trace of illegal drugs.
 - c. take money derived from an illegal activity and use it for gambling at a casino.
 - d. use illegal funds to finance terrorist activities.
 - e. none of the above

10. Bulk smuggling is the
 - a. movement of large amounts of cash
 - b. movement of large amounts of cash or monetary instruments
 - c. movement of large amounts of cash or monetary instruments, to or from U.S. borders
 - d. movement of large amounts of cash or monetary instruments, to or from U.S. borders, to evade currency reporting requirements.
 - e. movement of large amounts of cash or monetary instruments, to or from U.S. borders, to evade currency reporting requirements, and the source of the funds are from an illegal enterprise.

Test Your Learning answers are located in the Appendix.

APPENDIX: TEST YOUR LEARNING ANSWERS

Chapter 1: What is Privacy?

1. d
2. a
3. e
4. b
5. f
6. a, b, c, d, e
7. c
8. e
9. True
10. False. A search warrant is needed.

Chapter 2: Privacy Torts

1. a
2. b
3. c
4. d
5. c
6. b
7. c
8. e
9. a
10. d

Chapter 3: Privacy at Home

1. d
2. e
3. b
4. a
5. d
6. d
7. a
8. d
9. e
10. c


Chapter 4: Privacy Outside Home

- 1. d
- 2. c
- 3. c
- 4. a
- 5. a
- 6. d
- 7. c
- 8. d
- 9. a
- 10. a

I joined MITAS because
I wanted **real responsibility**

The Graduate Programme
for Engineers and Geoscientists
www.discovermitas.com







Month 16

I was a construction supervisor in the North Sea advising and helping foremen solve problems

Real work
International opportunities
Three work placements





Chapter 5: Privacy at Work

1. b
2. e
3. c
4. a
5. d
6. c
7. b
8. b
9. a
10. a

Chapter 6: Privacy and the Government

1. d
2. c
3. a
4. e
5. b
6. b
7. a
8. a
9. a
10. d

ENDNOTES

1. See <http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#616e124ddfbd>
2. See <https://en.oxforddictionaries.com/definition/privacy>
3. See <http://www.dictionary.com/browse/privacy>
4. Consistent with this premise, it is generally agreed that there are certain safe havens of privacy such as the inside of your home.
5. See <https://iapp.org/about/what-is-privacy/>
6. The author is the copyright holder of the image.
7. The full text of the article is available at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
8. Thomas Cooley appears to have coined the phrase “the right to be let alone” in his *Treatise on the Law of Torts* (1st ed. 1879): “Personal immunity – the right of one’s person may be said to be a right of complete immunity; the right to be alone.” At 29. Warren and Brandeis were careful to credit Cooley with this creation and cited the second edition of the treatise. Warren & Brandeis, *supra* note 1, at 195 n.4.
9. The full text of the article is available at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
10. A LEXIS search on September 1, 2016 indicates that the concept of privacy was actually discussed in earlier cases such as *Keene v. Wheatley*, 14 F. Cas. 180, 1861 U.S. App. LEXIS 377, 4 Phila. 157, 17 Legal Intel. 349, 9 Am. Law Reg. (1861) 33, 5 Pa. Law J. Rep. 501 (C.C.E.D. Pa. 1861). In *Keene*, the term privacy was used “it is, that the common law, in cases not aided or prejudiced by statute, shelters the privacy and seclusion of thoughts and sentiments committed to writing, and desired by the author to remain not generally known.” p. 201. In a different context, *Deery v. Cray*, 72 US (5 Wall) 795; 18 L Ed 653 (1867) discussed a Maryland law that required a married woman to present testimony privately, not in the presence of her husband. *United States v. Three Tons of Coal*, 28 F Cas 149 (ED Wis, 1875) mentions privacy in terms of search and seizure.
11. See <http://www.brandeis.edu/now/2013/july/privacy.html>
12. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/court-role-and-structure/comparing-federal-state-courts>
13. The federal courts and each state court have court rules that detail the process attorneys and the public must follow for the filing of court documents. Some courts such as the federal judiciary, have a separate set of rules for civil and criminal cases. Other courts may have rules for appellate courts. In addition, it is common practice both on the federal and state level to have written evidentiary rules that prescribe how evidence can be presented to a court.

14. According to the authors Ellen Alderman and Caroline Kennedy in their book *The Right to Privacy*, “(T) he word ‘privacy’ does not appear in the United States Constitution,” but “As most Americans believe the U.S. Constitution and/or Amendments specifically includes the word ‘privacy’ and protects privacy rights.”
15. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/educational-activities/first-amendment-activities>
16. See <https://constitutioncenter.org/interactive-constitution/amendments/amendment-iii>
17. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0>
18. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0>
19. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17. U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/educational-activities/fifth-amendment-activities>
20. See <https://www.whitehouse.gov/1600/constitution>
21. For an example, see the concurring opinion of Justice Goldberg in the case of *Griswold v. Connecticut* located at <http://law2.umkc.edu/faculty/projects/ftrials/conlaw/griswold.html>

ie business school

93%
OF MIM STUDENTS ARE
WORKING IN THEIR SECTOR 3 MONTHS
FOLLOWING GRADUATION

MASTER IN MANAGEMENT

- STUDY IN THE CENTER OF MADRID AND TAKE ADVANTAGE OF THE UNIQUE OPPORTUNITIES THAT THE CAPITAL OF SPAIN OFFERS
- PROPEL YOUR EDUCATION BY EARNING A DOUBLE DEGREE THAT BEST SUITS YOUR PROFESSIONAL GOALS
- STUDY A SEMESTER ABROAD AND BECOME A GLOBAL CITIZEN WITH THE BEYOND BORDERS EXPERIENCE

Length: 10 MONTHS
Av. Experience: 1 YEAR
Language: ENGLISH / SPANISH
Format: FULL-TIME
Intakes: SEPT / FEB

5 SPECIALIZATIONS
PERSONALIZE YOUR PROGRAM

#10 WORLDWIDE
MASTER IN MANAGEMENT
FINANCIAL TIMES

55 NATIONALITIES
IN CLASS

www.ie.edu/master-management | mim.admissions@ie.edu | [f](#) [t](#) [i](#) Follow us on IE MIM Experience

22. See <https://www.loc.gov/rr/program/bib/ourdocs/14thamendment.html> for additional information on the Fourteenth Amendment
23. This quote is from Section 1 of the Fourteenth Amendment. See <https://www.archives.gov/founding-docs/amendments-11-27>
24. In *Meyer*, it was a violation of state law to teach a language in a public or parochial school other than English until a child passed the eighth grade. A teacher taught German to a 10-year old student in a parochial school, with the consent of the child's parents. The teacher was found guilty of violating Nebraska law.
25. The full text of the Meyer v. Nebraska case is available at <https://supreme.justia.com/cases/federal/us/262/390/case.html>
26. See <https://www.oyez.org/cases/1900-1940/268us510>
27. Oral arguments for the case as well as the full opinion from the U.S. Supreme Court are available at *Griswold v. Connecticut*. (n.d.). Oyez. Retrieved February 17, 2017 from <https://www.oyez.org/cases/1964/496>
28. See <https://supreme.justia.com/cases/federal/us/381/479/case.html>
29. See 381 U.S. 481–486.
30. The full text of the case is available at <https://www.oyez.org/cases/1964/496>
31. The author is the copyright holder of the image.
32. See <https://supreme.justia.com/cases/federal/us/405/438/case.html>
33. See <https://www.oyez.org/cases/1971/70-17/>
34. See 405 U.S. 453.
35. See <https://www.oyez.org/cases/1971/70-18>
36. Ibid.
37. Ibid.
38. See <https://www.oyez.org/cases/1967/35>
39. See <https://supreme.justia.com/cases/federal/us/389/347/case.html>
40. See <https://www.oyez.org/cases/1967/35>
41. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>
42. See <https://www.oyez.org/cases/2012/12-207>
43. See <https://www.oyez.org/cases/2000/99-8508>
44. See <https://www.oyez.org/cases/2011/10-1259>
45. Ibid.
46. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.supremecourt.gov/opinions/09pdf/08-1332.pdf>
47. See <https://www.oyez.org/cases/2009/08-1332>
48. See <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx>

49. A crime is an offense against the state where the government is the prosecuting party. Punishment in crimes can include incarceration, fines, and community service.
50. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/court-role-and-structure/comparing-federal-state-courts>
51. For example, in the State of Michigan courts can award exemplary damages. See http://www.legalreforminthenews.com/Tort%20Profiles/MI_Tort_Laws.html
52. See <http://legal-dictionary.thefreedictionary.com/exemplary+damages>
53. See <http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html>
54. See <https://concurringopinions.com/archives/2010/03/william-prosser-and-the-privacy-torts.html>
55. Privacy torts are located in *Restatement of Torts*, Second §§ 652A-E (1997). See https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm
56. The author is copyright holder of the image.
57. The author is copyright holder of the image.
58. The author is copyright holder of the image.
59. The author is copyright holder of the image.
60. The author is copyright holder of the images.
61. The author is copyright holder of the image.
62. The author is copyright holder of the image.
63. See https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm
64. The author is copyright holder of the image.
65. See <https://dockets.justia.com/docket/pennsylvania/paedce/2:2010cv00665/347863>
66. See the Paragraph 2 in the Complaint filed in the *Robbins et al v. Lower Merion School District* available at https://www.pacermonitor.com/view/6LZS7RA/ROBBINS_et_al_v_LOWER_MERION_SCHOOL_DISTRICT_et_paedce-10-00665_0001.0.pdf
67. See the Complaint filed the *Robbins et al v. Lower Merion School District* case available at <https://docs.justia.com/cases/federal/district-courts/pennsylvania/paedce/2:2010cv00665/347863/93>
68. See Paragraph 17 in <https://docs.justia.com/cases/federal/district-courts/pennsylvania/paedce/2:2010cv00665/347863/1>
69. See <http://www.cbsnews.com/news/610k-settlement-in-school-webcam-spy-case/>
70. See 890 F.Supp.2d 1325 (2012).
71. The full text of this case is available at <http://caselaw.findlaw.com/ga-supreme-court/1626940.html>
72. Ibid.
73. Ibid.
74. Ibid.
75. See the Georgia Supreme Court's opinion at <http://law.justia.com/cases/georgia/supreme-court/2013/s12q2087.html>
76. See https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm
77. See <http://www.forbes.com/dead-celebrities/#b53f0576a518>
78. See [facebook.com/duanereade](https://www.facebook.com/duanereade)

79. The entire Complaint can be found at http://online.wsj.com/public/resources/documents/0410_heiglsuit.pdf
80. See <http://blogs.wsj.com/law/2014/04/10/will-katherine-heigls-tweet-lawsuit-against-duane-reade-hold-up-in-court/>
81. Ibid.
82. FOIA refers to the Freedom of Information Act. There is a federal version and state versions of the law, which require governmental agencies to produce certain types of information upon written request. This topic is discussed later in the book in Chapter Six.
83. See Jobs's Job, *ECONOMIST*, Aug. 2, 2008, at 68 (discussing the effect of Jobs's health on Apple's financial outlook).
84. Ibid.
85. See <https://www.hhs.gov/hipaa/>
86. See <http://www.dmlp.org/legal-guide/virginia-false-light>
87. The author is copyright holder of the image.
88. See *Silverman v. United States*, 365 U.S. 505, 511 (1961).
89. The full text of *Mapp v Ohio*, 367 U.S. 643 (1961) is available at <https://supreme.justia.com/cases/federal/us/367/643/case.html>
90. See <https://supreme.justia.com/cases/federal/us/367/643/case.html>
91. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/supreme-court-landmarks/mapp-v-ohio-podcast>



"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

92. See <https://www.oyez.org/cases/2000/99-8508>
93. Ibid.
94. Ibid.
95. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/supreme-court-landmarks/mapp-v-ohio-podcast>
96. See <https://supreme.justia.com/cases/federal/us/466/170/> for the full text of *Oliver*.
97. See footnote 12 in *Oliver v. United States*, (1984) 466 U.S. 170 referencing p.182.
98. See https://www.supremecourt.gov/opinions/12pdf/11-564_5426.pdf for the full text of *Jardines*.
99. See <http://blog.constitutioncenter.org/2015/04/supreme-court-settles-latest-fourth-amendment-dog-sniff-case/>
100. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/supreme-court-landmarks/mapp-v-ohio-podcast>
101. The author is copyright holder of the image.
102. The author is copyright holder of the image.
103. See *United States v. Thompson*, 667 F. Supp. 2d 758 (S.D. Ohio 2009).
104. See “Riley v. California.” *Oyez*. Chicago-Kent College of Law at Illinois Tech, n.d. Dec 8, 2016 available at <https://www.oyez.org/cases/2013/13-132>
105. Ibid.
106. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/supreme-court-landmarks/mapp-v-ohio-podcast>
107. The author is the copyright holder of the image.
108. See *United States v. Causby*, 328 U.S. 256 (1946).
109. See <https://www.l-wlaw.com/drone-new-drone-regulations-open-door-droning/>
110. The author is the copyright holder of the image.
111. See <https://www.oyez.org/cases/1988/87-764>
112. Ibid.
113. See <https://www.law.cornell.edu/uscode/text/49/40103>
114. See <https://www.wsj.com/articles/drones-boom-raises-new-question-who-owns-your-airspace-1431535417>
115. Note that the legal standards for minors are different than for adults, and parental or guardian permission is needed to publically display photos of minors.
116. See <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>
117. Verifiable consent can include responding to a toll free number, signing and returning a consent form, the use of a credit or debit card to verify identification, or providing a government ID.
118. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>

119. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>, p. 3
120. See <http://tektreeinc.com/internet-of-things>
121. Ibid.
122. See <http://www.nbcnews.com/health/health-news/insulin-pump-vulnerable-hacking-johnson-johnson-warns-n659221>
123. See <https://www.animas.com/diabetes-insulin-pump-and-bloog-glucose-meter/onetouch-ping-blood-glucose-monitor>
124. In early 2017, it was reported that the product line was acquired from St. Jude Medical to Abbott Laboratories. See <http://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/>
125. The author is the copyright holder of the image.
126. See <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>
127. See <https://www.theguardian.com/technology/2016/mar/13/autonomous-cars-self-driving-hack-mikko-hypponen-sxsw>
128. See <http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>
129. See <https://msu.allclearid.com/>
130. This is an email sent to the author.
131. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.uscourts.gov/about-federal-courts/educational-resources/supreme-court-landmarks/mapp-v-ohio-podcast>
132. The author is copyright holder of the image
133. See https://www.wsgl.com/attorneys/BIOS/PDFs/boring_v_google.pdf
134. Privacy legal standards for minors are different than for adults, and parental or guardian permission is needed to publically display photos of minors that can identify them.
135. The author is the copyright holder of the image.
136. See <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
137. Ibid.
138. See <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html>
139. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://nces.ed.gov/pubs2011/2011601.pdf>
140. See <https://www.law.cornell.edu/cfr/text/34/99.31>. This website contains the text of 34 CFR § 99.31. This citation refers to Title 34 of the Code of Federal Regulations at section 99.31. The Code of Federal Regulations is an administrative code that provides operating rules for federal agencies.
141. See <http://familypolicy.ed.gov/content/ferpa-general-guidance-parents>
142. See <http://familypolicy.ed.gov/sites/fpco.ed.gov/files/for-parents.pdf> on pages 3 and 4.
143. Author is the copyright holder of the image.

144. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www2.ed.gov/policy/gen/guid/fpco/index.html>
145. See <http://www2.ed.gov/policy/gen/guid/fpco/courtcases/owasso.html>
146. See *Owasso*, 2002, p. 434–435 available at <https://www.law.cornell.edu/supct/html/00-1073.ZS.html>
147. See <https://www.law.cornell.edu/supct/html/00-1073.ZS.html>
148. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://supreme.justia.com/cases/federal/us/534/426/case.html>
150. See <https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/>
151. See <https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html?language=es>
152. See <https://www.healthit.gov/providers-professionals/faqs/are-there-penalties-providers-who-don%E2%80%99t-switch-electronic-health-record>
153. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.healthit.gov/providers-professionals/faqs/are-there-penalties-providers-who-don%E2%80%99t-switch-electronic-health-record>
154. This material is in the public domain in the United States as it is the work of the University of Groningen federal government and available for use under 17 U.S.C. § 105. Source: <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html?language=es>

Excellent Economics and Business programmes at:



**university of
 groningen**




**“The perfect start
 of a successful,
 international career.”**

CLICK HERE
 to discover why both socially
 and academically the University
 of Groningen is one of the best
 places for a student to be

www.rug.nl/feb/education

155. See 45 CFR § 103 available at http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr160_main_02.tpl
156. See <http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
157. See <https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html?language=es>
158. See <http://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html>
159. See <http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>
160. The author is the copyright holder of the image.
161. See <https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html?language=es>
162. See <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/>
163. See <https://www.healthit.gov/providers-professionals/electronic-medical-records-emr>
164. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.healthit.gov/policy-researchers-implementers/hitech-programs-advisory-committees>
165. See <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html>
166. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/HITECH/index.html>
167. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
168. In answer to the question, the company is not a medical care provider under federal law and has now compliance requirement.
169. The author is copyright holder of the image.
170. See <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>
171. See <https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003>
172. See <http://www.federalreservehistory.org/Events/DetailView/53>
173. See 15 U.S.C. § 1681 available at <https://www.law.cornell.edu/uscode/text/15/1681>
174. See <https://www.equifax.com/personal/>
175. See <https://www.transunion.com/>
176. See <http://www.experian.com/>
177. See <https://connect.experian.com/legal/fcra-obligations.html>
178. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>
179. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.consumer.ftc.gov/articles/0384-sample-letter-disputing-errors-your-credit-report>
180. See <https://www.identitytheft.gov/#what-to-do-right-away>

181. See <https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003>
182. See <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>
183. In answer to the question, both parties can file a fraud alert. The checking account and funds belonged to Mrs. Gray and the check was stolen from her. Her daughter Colleen's signature was forged, so she also can file a fraud alert.
184. See <https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes>
185. See <https://www.identitytheft.gov/#what-to-do-right-away>
186. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>
187. See <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>
188. See <http://www.federalreservehistory.org/Events/DetailView/53>
189. See <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>
190. See Section 4(k) provisions and regulations on financial activities at <https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf>
191. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>
192. See <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>
193. See <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>
194. See <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>
195. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>
196. See <https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business>
197. See <https://ourdocuments.gov/doc.php?flash=false&doc=100>
198. See 11 CFR § 110.4(c) available at <https://www.law.cornell.edu/cfr/text/11/110.4>
199. See <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>
200. Ibid.
201. See <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>
202. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.ftc.gov/tips-advice/business-center/guidance/using-consumer-reports-what-employers-need-know>
203. See <https://www.dol.gov/general/topic/disability/ada>
204. See <https://www.eeoc.gov/facts/jobapplicant.html>

205. See https://www.ada.gov/2010_regs.htm
206. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.dol.gov/whd/polygraph/>
207. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.dol.gov/whd/regs/compliance/posters/eppa.htm>
208. The author is the copyright holder of the image.
209. See p. 101 located at https://cyber.harvard.edu/privacy/smyth_v_pillsbury.htm
210. See a recent Massachusetts Superior Court decision, Falmouth Firefighters Union v. Town of Falmouth, which is consistent with the Smyth ruling located at <https://www.employmentmattersblog.com/2012/05/no-expectation-of-privacy-in-emails-sent-over-employers-email-account-massachusetts-court-decides/>
211. The FCRA disposal rule applies to “(c)redit reports and credit scores are consumer reports. So are reports businesses or individuals receive with information relating to employment background, check writing history, insurance claims, residential or tenant history, or medical history. See <https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how>
212. See <https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how>
213. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/aam/drug_alcohol

American online

LIGS University

is currently enrolling in the
Interactive Online **BBA, MBA, MSc,**
DBA and PhD programs:

- ▶ enroll **by September 30th, 2014** and
- ▶ **save up to 16%** on the tuition!
- ▶ pay in 10 installments / 2 years
- ▶ Interactive Online education
- ▶ visit www.ligsuniversity.com to find out more!

Note: LIGS University is not accredited by any nationally recognized accrediting agency listed by the US Secretary of Education. More info [here](#).



214. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.fbijobs.gov/working-at-FBI/eligibility>
215. See 5 U.S.C. § 552a.
216. See <https://www.justice.gov/opcl/privacy-act-1974>
217. See 5 U.S.C. § 552. Note that the federal law only covers federal agencies, and each state has their own version of a FOIA law.
218. See <https://www.archives.gov/st-louis/military-personnel/foia-info.html>
219. The full text of the law is available at [https://www.legislature.mi.gov/\(S\(jjucqbquewlstmksoizsx2n\)\)/documents/mcl/pdf/mcl-act-397-of-1978.pdf](https://www.legislature.mi.gov/(S(jjucqbquewlstmksoizsx2n))/documents/mcl/pdf/mcl-act-397-of-1978.pdf)
220. See <https://www.eeoc.gov/laws/statutes/gina.cfm>
221. Ibid.
222. See <https://www.eeoc.gov/eeoc/publications/fs-gina.cfm>
223. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www1.eeoc.gov/eeoc/newsroom/release/1-7-16.cfm>
224. See <https://www.supremecourt.gov/opinions/09pdf/08-1332.pdf>
225. See <https://www.gpo.gov/fdsys/pkg/PLAW-107publ56>
226. The author is the copyright holder of the image.
227. See <https://www.justice.gov/opcl/privacy-act-1974>
228. See <https://www.justice.gov/opcl/introduction>
229. See the full text of the report at <https://www.ncjrs.gov/pdffiles1/Digitization/49602NCJRS.pdf>
230. See <https://www.justice.gov/opcl/computer-matching>
231. Comments from the *Federal Register* regarding changes to this law are available at http://itlaw.wikia.com/wiki/OMB_Privacy_Act_Implementation,_Guidelines_and_Responsibilities
232. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#need>
233. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#required>
234. See Privacy Commission Report at 517–18, available at <http://epic.org/privacy/ppsc1977report>
235. See OMB Guidelines, 40 Fed. Reg. 56,741, 56,742 (Dec. 4, 1975), available at https://iapp.org/media/pdf/resource_center/omb_circular_a_108_12_12_16.pdf
236. See OMB Guidelines, 40 Fed. Reg. 28,948, 28,954 (July 9, 1975), linked at <https://www.justice.gov/opcl/role-office-managementand-budget>
237. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: http://www.census.gov/about/policies/foia/privacy_act_requests.html
238. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#research>
239. See <http://www.bls.gov/news.release/prod2.nr0.htm>
240. See OMB Guidelines, 40 Fed. Reg. 28,948, 28,955 (July 9, 1975), linked at <https://www.justice.gov/opcl/role-office-managementand-budget>
241. See <https://www.archives.gov/research/military/veterans/online.html>

242. See OMB Guidelines, 40 Fed. Reg. 28,948, 28,955 (July 9, 1975), linked at <https://www.justice.gov/opcl/role-office-managementand-budget>
243. See <http://statepatrol.ohio.gov>
244. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#health>
245. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#congress>
246. See <http://www.gao.gov/about/> for more information about the General Accounting Office.
247. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#general>
248. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#court>
249. See <https://www.justice.gov/opcl/conditions-disclosure-third-parties#debt>
250. See <https://www.justice.gov/opcl/ten-exemptions>
251. Ibid.
252. See the case of *FAA v Cooper*, 566 U. S. ____ (2012) at <https://www.supremecourt.gov/opinions/11pdf/10-1024.pdf>
253. Compiled from <https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>
254. See <https://www.justice.gov/archive/ll/highlights.htm>
255. See <https://www.fdic.gov/regulations/examinations/bsa/PATRIOT-Act.pdf>
256. See <https://www.irs.gov/businesses/small-businesses-self-employed/report-of-cash-payments-over-10000-received-in-a-trade-or-business-motor-vehicle-dealership-qas>
257. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.sec.gov/about/offices/ocie/amlsourcetool.htm>
258. See 31 U.S.C. §§ 5316 and 5317 for details on the reporting requirements for bulk cash transactions.
259. See <https://www.law.cornell.edu/uscode/text/31/5332> for the full text of this section.
260. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.ice.gov/news/releases/hsi-bulk-cash-smuggling-task-force-seizes-nearly-3-million-illicit-proceeds-third-year>
261. See <https://judiciary.house.gov/press-release/goodlatte-applauds-passage-bill-protect-fourth-amendment-digital-age/>
262. See <https://it.ojp.gov/privacyliberty/authorities/statutes/1285>
263. Ibid.
264. See <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119>
265. Ibid.
266. See <https://it.ojp.gov/privacyliberty/authorities/statutes/1285>
267. See 18 U.S.C. §§ 2701–12.
268. See <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>
269. See <https://www.law.cornell.edu/uscode/text/18/part-II/chapter-206>
270. See <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>
271. Ibid.
272. Ibid.
273. See <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286>

274. For detailed information about the operation of the court see <http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court>
275. See <http://www.fisc.uscourts.gov/>
276. See <http://www.fisc.uscourts.gov/FISCR>
277. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court>
278. See <https://archives.fbi.gov/archives/news/testimony/usa-patriot-act-amendments-to-foreign-intelligence-surveillance-act-authorities>
279. See <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282>
280. See <https://www.gpo.gov/fdsys/pkg/CRPT-112srpt13/pdf/CRPT-112srpt13.pdf>
281. See <https://judiciary.house.gov/issue/usa-freedom-act/>
282. See <http://www.fisc.uscourts.gov/>
283. See <https://www.tsa.gov/travel/security-screening>
284. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.tsa.gov/travel/security-screening>
285. See <https://www.tsa.gov/travel/security-screening>
286. Ibid.
287. See <http://www.usatoday.com/story/news/2016/08/10/dea-travel-record-airport-seizures/88474282/>
288. See <https://wikileaks.org/>



DON'T EAT YELLOW SNOW

What will your advice be?

Some advice just states the obvious. But to give the kind of advice that's going to make a real difference to your clients you've got to listen critically, dig beneath the surface, challenge assumptions and be credible and confident enough to make suggestions right from day one. At Grant Thornton you've got to be ready to kick start a career right at the heart of business.

Sound like you? Here's our advice: visit GrantThornton.ca/careers/students

Scan here to learn more about a career with Grant Thornton.



 **Grant Thornton**
An instinct for growth™

© Grant Thornton LLP. A Canadian Member of Grant Thornton International Ltd

289. See <https://wikileaks.org/What-is-Wikileaks.html>
290. Ibid.
291. See <https://wikileaks.org/dnc-emails>
292. See <https://wikileaks.org/Statement-on-Bradley-Manning-Case.html>
293. See <https://wikileaks.org/-Leaks-.html>
294. See <http://www.newsweek.com/how-much-did-snowden-take-not-even-nsa-really-knows-253940>
295. See https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html?utm_term=.074b7ec4fcde
296. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <http://www.documentcloud.org/documents/716888-u-s-vs-edward-j-snowden-criminal-complaint.html>
297. This material is in the public domain in the United States as it is the work of the United States federal government and available for use under 17 U.S.C. § 105. Source: <https://www.foia.gov>
298. See <https://www.foia.gov/faq.html#cost>
299. See <https://www.foia.gov/faq.html#exemptions>
300. See <https://www.foia.gov/faq.html#cost>
301. See <https://publications.usa.gov/epublications/foia/letters.htm>
302. See <https://publications.usa.gov/epublications/foia/letters.htm>