

Business law

Prepared by Dr. Galal Elmasry

MGM412

Lecture 7



Business law

Lecture 7

MGM412

Prepared by
Dr. Galal Elmasry

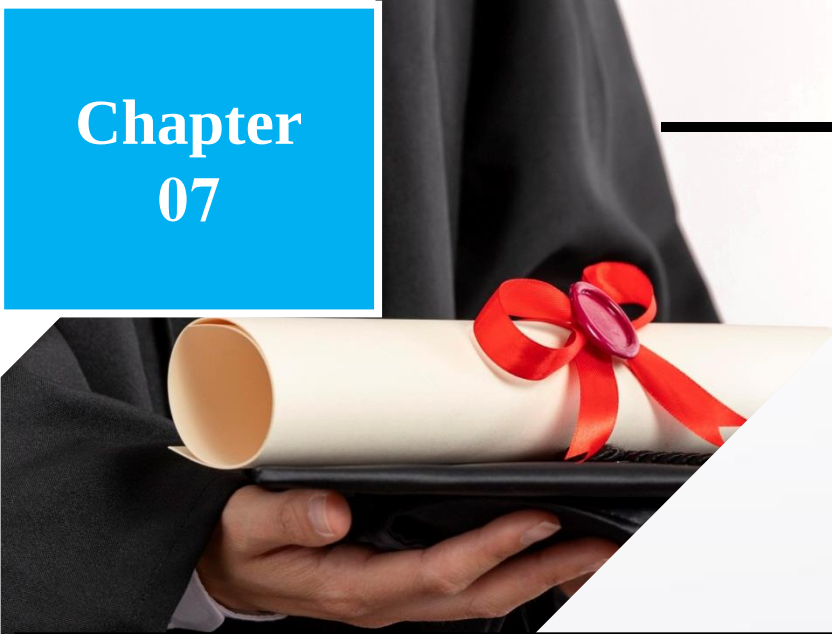
www.midocean.ae

Chapter 7 :Workplace Privacy and Information Security:

The most important main themes of the lecture:

- 1- Introduction.
- 2- Right to Privacy.
- 3- Workplace Privacy.
- 4- Information Security Issues.
- 5- Concluding Thoughts.

1- Introduction:



- Privacy is a fundamental right of individuals that is often compromised by government and businesses. Sometimes individuals and businesses voluntarily give up their privacy rights, without considering the consequences of doing so. Workplace privacy and information security is a fast growing area of the law that has important implications across industries.

-Privacy is the right of a person or person's property to be free from unwarranted public scrutiny or exposure. In other words, it is the right to personal autonomy and to express oneself selectively. Privacy includes both bodily integrity and the protection of confidential information, including medical and financial records.

1-Implied Constitutional Right:

Privacy is an implied Constitutional right, meaning it is a right based on the “zones of privacy” created by the US Constitution. However, the word “privacy” is not in the Constitution itself.

The right to privacy was first mentioned in a Harvard Law Review article in 1890 by Samuel Warren and Louis Brandeis, who later served on the US Supreme Court from 1916 until 1939. Warren and Brandeis argued the right to privacy is an important civil liberty which should not be violated by sensational journalists and developments in technology.

- The technology in the late 1890s they were the most concerned with was photography and telephones. In particular, they were concerned about people losing their right to privacy when others take photographs of them or listen to their conversations.
- Privacy was discussed in the legal community for 75 years before the US Supreme Court expressly held individuals have a Constitutional right to privacy in the 1965 Griswold v. Connecticut decision.
- Privacy cases involve different circumstances, such as the right to choose whether to marry and to whom, the right to choose whether to have children, and the right to protect confidential information such as medical and financial records.

-The Framers of the Constitution did not include the word “privacy” in the Constitution but it is a fundamental right underlying the core tenets of the document.

The Bill of Rights begins by recognizing fundamental rights that are essential to an individual’s identity: speech, religion, press, assembly, and petition for redress from the government. From there, the Bill of Rights expands protection of individuals to include their homes and possessions. For example, the Fourth Amendment prohibits unreasonable searches and seizures by the government. As reflected in the Bill of Rights, privacy is an essential right the Constitution intends to protect.

-When analyzing privacy cases, courts ask whether an individual has a reasonable expectation of privacy. To establish a “reasonable expectation of privacy,” a person must meet two requirements:

1. The individual has an actual, subjective expectation of privacy. In other words, did that particular person think he or she was doing something in private that others could not observe?
2. Society accepts the individual’s expectation of privacy as reasonable. In other words, as a community do we expect those circumstances to be private?

- This legal test has both a subjective and objective standard. If an individual does not expect their actions to be private, then no right to privacy exists under the circumstances. Similarly, if society as a whole does not expect to have privacy under the circumstances, it does not matter what the individual may personally believe, no right of privacy exists.

-**For example,** if a person calls her doctor to discuss medical test results, then she has a subjective expectation of privacy. If she calls her doctor from her home, then she has an objective expectation of privacy because society recognizes the right of people to have private conversations in their own homes. **However,** if she has the conversation on her cell phone while riding the bus, then she does not have a right to privacy because it is not objectively reasonable to expect privacy on public transportation.

2- Statutes:

- Congress and state legislatures have also passed various laws to protect the privacy of individuals and their property. Some of the most important federal laws related to workplace privacy are discussed below.

2- Statutes:

- There is a growing trend among states to require internet service providers to obtain consent from consumers before sharing any of their personal information, including websites visited and consumer habits.
- Businesses engaged in e-commerce with residents of California must post their privacy policy conspicuously on their websites and abide by their policies. California law also requires disclosure of consumer software tracking policies.

3- International Law:

- The right to privacy is contained in Article 12 of the Universal Declaration of Human Rights, which was adopted in 1948 in response to the horrors of World War II. The Universal Declaration of Human Rights states:

- No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.

The Universal Declaration of Human Rights has been adopted by the majority of nations, including the United States.

- Many other bilateral treaties and conventions recognize the right to privacy in various circumstances. Currently, about 150 nations recognize privacy as part of their international legal obligations. However, enforcement of the right to privacy is inconsistent across nations.

3- Workplace Privacy:

- Employees generally do not have a reasonable expectation of privacy in the workplace, especially when using company equipment or when the employer has a policy stating employees may be monitored. However, some areas such as employee restrooms and locker rooms may not be monitored. Courts have held employees do not give up all expectations of privacy by the nature of their employment. Therefore, employers should ensure that they limit monitoring activities to reasonable places where the employer has a legitimate business interest for doing so.

3- Workplace Privacy:

1- Hiring Process:

- Employers often run background checks on prospective employees as part of their hiring process. Depending on what type of background check is done and the information used, a range of privacy issues are involved. Some states regulate the type of documents that a prospective employer may consider when making hiring decisions. Businesses need to ensure they comply with all state laws where they hire employees.
- The use of artificial intelligence (AI) is a growing trend in recruiting and hiring. AI is often used to review resumes, applications, and publicly available social media. AI-powered video-interview platforms apply algorithms to video-recorded interviews to facilitate an employer's assessment of applicants.

3- Workplace Privacy:

2- Drug and Alcohol Testing:

- Employers with drug and alcohol testing policies are highly regulated by the states where they operate. State requirements vary about required notice of testing, the nature and location of testing, and when testing may occur. All states protect employee privacy regarding who receives the test result and how those results are to be collected, stored, and destroyed. Employers who engage in drug and alcohol testing need to be informed about the legal consequences of enforcing their policies.

-Employees frequently challenge drug and alcohol testing as a violation of their right to privacy. Employers generally win these lawsuits when:

- The employer complies with all state requirements for drug and alcohol testing;
- Conducts the test with the employee's consent;
- Conducts the test in a manner that was not offensive;

3- Workplace Privacy:

- The test results do not reveal information unrelated to the purpose of the test.
- Employers must be careful to limit disclosure of test results to only those with a need to know. Businesses may lawfully conduct a drug or alcohol test but still be liable for privacy violations based on how they handled the results.

2- Health Insurance Portability and Accountability Act:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) seeks to protect confidential health information and mandates standards for handling such information. HIPAA has a Privacy Rule regulating the use and disclosure of individually identifiable health information. The Privacy Rule protects Protected Health Information (PHI) , which includes all information related to the past, present or future health status of an identified individual, of treatment received, or of payment for treatment. PHI also includes billing records, information about premium payments, and enrollment information.

3- Workplace Privacy:

2- Health Insurance Portability and Accountability Act:

-As a result, PHI includes medical information required by employers to carry out their obligations under the Americans with Disabilities Act, the Family Medical Leave Act, workers' compensation, drug testing, and employer-sponsored health care plans.

- HIPAA also has a Security Rule to ensure the confidentiality, integrity and availability of electronic PHI. Under the Security Rule:

- Confidentiality means PHI is not made available or disclosed to unauthorized individuals or processes;
- Integrity means PHI is not altered or destroyed in an unauthorized manner;
- Availability means PHI is accessible and usable upon demand by an authorized individual.

3- Workplace Privacy:

3- Electronic Monitoring:

- Federal law and most state laws allow employers to monitor their employees' electronic communications occurring over the employer's hardware, software, and servers. If the employer provides the computer system, the employer has the right to monitor electronic communications on the system, even if those communications are not work related.
- Employers may also monitor communications when employees consent to the monitoring. Therefore, many employers require employees to sign a waiver consenting to private communications sent via the employer's equipment to be monitored. This helps defend against invasion of privacy claims better than having a policy in the employee handbook alone.

3- Workplace Privacy:

3- Electronic Monitoring:

- Businesses may also monitor conversations with customers in the ordinary course of business as long as they give notice. As a result, many customer service lines use a recorded message that “this call may be monitored for training purposes” before customers are connected to a customer service agent.
- The most important federal law regarding monitoring of electronic communications is the Electronic Communications Privacy Act (ECPA), which was passed by Congress in 1986. ECPA has two parts. The first part is known as the Wiretap Act and the second as the Stored Communications Act. ECPA prohibits the acquisition of the content of a wire, oral or electronic communication using an electronic, mechanical or other device. ECPA also prohibits the use or disclosure of an unlawfully intercepted communication.

3- Workplace Privacy:

4- Workplace Recordings:

- Although recordings may be useful to capture the content of a conversation, recordings pose legal and business risks to employers. Both employers and employees may violate federal and state wiretapping laws by recording conversations without consent of the other parties. Even with consent, businesses that engage in recording employees and customers damage employee morale and risk losing customers.
- Twelve states prohibit recording a conversation unless all parties consent. The majority of states allow customers and employees to hold a business liable for wiretapping violations under the respondeat superior doctrine. As a result, businesses may be liable for their employees' unlawful recordings if done in the course and scope of employment or done to help the business.

3- Workplace Privacy:

-State and federal wiretapping laws carry both civil and criminal penalties. Many state laws provide for treble damages or a statutory damage amount. Federal wiretapping laws impose fines up to one hundred dollars per day or ten thousand dollars, whichever is greater.

5- Social Media:

-An employer's right to monitor electronic communications generally does not include social media. As a result, employers are not entitled to monitor social media accounts through coercion or deceit. For example, an employer cannot require employees to provide passwords to their social media accounts. Employers also cannot log onto the social media accounts of others (including employees) and pose as them to see private accounts.

- **However**, if social media accounts are public, then employers are entitled to review them to the same extent as other members of the public.

3- Workplace Privacy:

6-Videotaping and Surveillance Cameras:

- ECPA only protects electronic communications. **As a result**, ECPA does not apply to video or camera surveillance without an audio component. To avoid violating ECPA, businesses should ensure their security and surveillance cameras do not capture human voices.
- Security cameras cannot be used in areas in which employees and customers have a reasonable expectation of privacy. **For example**, retailers cannot use cameras in changing rooms, restrooms, and locker rooms. Businesses need to place cameras so that private activity cannot, and is not, monitored and recorded.
- Businesses engaged in surveillance must use the most limited means available to conduct the surveillance. Companies should have a legitimate business reason to use security cameras, and they need to ensure the surveillance is targeted and limited in duration and scope.
- Retailers who use cameras to prevent theft at entryways and cash registers should place cameras in positions that are open and obvious to act as notice to customers. Signs giving express notice are also a best practice to avoid legal liability.

4-Information Security Issues:

-Information security is one of the fastest growing areas of the law affecting businesses today. Any business that collects, uses, and stores personal information about employees and customers is subject to these laws. Businesses are also increasingly targeted by hackers who seek to steal private information on a large scale.

1- Security Analysis:

- A simple but widely-used security model is the CIA Principle or CIA Security Rule, which stands for Confidentiality, Integrity and Availability. The principle is applicable across points of contact from access to a user's internet history to security of encrypted data across the Internet.

4-Information Security Issues:

1- Security Analysis:

- Confidentiality is the ability to hide information from those without authorization to view it. While perhaps the most obvious principle, it is usually the one that is attacked most often. Cryptography and Encryption are methods used to protect confidentiality of data transferred across the Internet.
- Integrity is the ability to ensure that data is an accurate and unchanged representation of the original information. One common security attack is to intercept some important data and make changes to it before sending it on to the intended receiver.
- Availability is the ability to make information readily accessible to authorized users at all times. Some security attacks attempt to deny access.

4-Information Security Issues:

2- Data Breaches:

- According to the Pew Research Center, almost eighty-five percent of individuals in the US shop online. And most retailers collect customer's personal and financial data. If a customer uses a form of payment other than cash, then the customer's personal and financial information will be shared with the business.

Rather than pickpocket an individual consumer, thieves today are targeting businesses to collect personal and financial information of entire consumer sets. Data breaches affect all industries, such as retail, credit bureaus, hospitals, and government agencies. In the first half of 2019, there were over 4.1 billion compromised documents reported as part of only 3,800 disclosed data breaches.

4-Information Security Issues:

2- Data Breaches:

- Cybersecurity experts advise that cyber criminals run automated online scripts looking for unsecured databases. While some larger businesses are particularly targeted, cyber criminals are the most successful when targeting small to medium-sized businesses that are unaware of the threat or do not want to spend adequate resources on cybersecurity. Businesses should be aware, though, that approximately sixty percent of data breaches are the result of human error rather than outdated or insufficient technology. Therefore, by adequately training employees, many data breaches may be avoided. For example, breaches often result from sending emails to the wrong person, responding to phishing attacks, sharing passwords, and leaving computer screens open.

4-Information Security Issues:

3-Big Data:

- In addition to financial data, businesses collect personal information about consumers and their habits. This is called big data. Consumer information is very valuable because businesses can search the data to identify spending habits to target marketing to likely customers. This reduces costs and increases profit for businesses, especially as e-commerce increases the number of competitors across industries.
- Another benefit to mining the data available about consumers is businesses can make more profitable decisions. For example, health insurance companies are heavily invested in big data because they want information about the lifestyle habits of the people they insure and potentially insure.

4-Information Security Issues:

3-Big Data:

- If they know someone is a smoker, eats a lot of sugary foods, or has a sedentary lifestyle, then they can adjust premiums accordingly to minimize their risk. Insurance companies look for trends not just for individuals but also regions, types of occupations (including those with the highest risk of addiction or obesity), and socio-economic status.
- Big data is also connected to the Internet of Things. The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. In other words, the IoT includes everyday devices connected to the internet, including medical devices, appliances, vehicles, and buildings.

4-Information Security Issues:

4-Transborder Data Transfers:

- As discussed previously, the EU has a comprehensive set of privacy laws and regulations. The EU has strict limits on the export of all human resources data and consumer information to the US, even when the data export occurs within the same business. To help US businesses comply with the EU laws, the US Department of Commerce negotiated a “safe harbor” of data protection practices that the EU approved. If a US business can certify its compliance with the Safe Harbor Principles, then the EU will approve data transfers to that business.

4-Information Security Issues:

5-Security Incident Preparation and Response:

-Businesses are not able to prevent all data security breaches. However, businesses need to take steps to protect against known and reasonably anticipated threats to confidential information. For businesses without sufficient in-house cybersecurity staff or expertise, Managed Security Service Providers (MSSPs) offer a wide range of security services, including setting up security infrastructure and incident response.

-Although federal and state laws vary regarding legal requirements, a business should have a written cybersecurity program that conforms to their industry's recognized cybersecurity framework.

4-Information Security Issues:

5-Security Incident Preparation and Response:

-In general, a cybersecurity program should:

- Protect the security and confidentiality of all electronically stored records containing an employee or customer's social security number, driver's license number, state identification card number, credit and debit card information, dates of birth, passwords, and personal information;
- Protect against any anticipated threats or hazards to the security or integrity of the confidential information;
- Provide for reliable and accurate backups of data; and
- Protect against unauthorized access to and acquisition of information likely to result in an employee or customer being exposed to a material risk of identity theft or fraud.

5-Concluding Thoughts:

- The internet and technology are changing the world at an incredibly fast pace. With those changes come the challenges to individuals and businesses to maintain privacy and protect personal information. Privacy is an implied Constitutional right deeply impacted by the use of technology. Regardless of type of industry, businesses need to have adequate cybersecurity policies and practices in place to protect confidential business, employee, and customers information.



Thank You