College: INDUSTRIAL TECHNOLOGY
Campus: Bambang Campus

DEGREE PROGRAM	**BS INFORMATION TECHNOLOGY**	**COURSE NO.**	**ITPC 13**				
SPECIALIZATION	Network Management and Security / Web and Mobile Development	**COURSE TITLE**	**SOCIAL ISSUES AND PROFESSIONAL PRACTICE**				
YEAR LEVEL	**4**	**TIME FRAME**	**3 hrs**	**WK NO.**	**5**	**IM NO.**	5

I. UNIT TITLE/CHAPTER TITLE

ANONYMITY, SECURITY AND PRIVACY

II. LESSON TITLE

1. Anonymity
2. Security
3. Privacy

III. LESSON OVERVIEW

This lesson surveys the traditional ethical issues of privacy, security, and anonymity and analyzes how these issues are affected by computer technology.

IV. DESIRED LEARNING OUTCOMES

At the end of the lesson, the students should be able to:

1. analyze stated security procedures for “weak points” that an attacker could exploit and explain how they could (or will) fail;
2. describe current computer-based threats to privacy; and
3. explain how the Internet may change the historical balance in protecting freedom of expression

V. LESSON CONTENT

1. Anonymity (Jerry, Jayson)

The Greeks used the $\alpha\nu\ \nu\upsilon\mu\ \alpha$ word to describe the state of being nameless. Anonymity is being nameless, having no identity. Since it is extremely difficult for anybody to live a meaningful life while one is totally anonymous, there are types of anonymity that people usually use.

Types:

- Pseudo-identity: An individual is identified by a certain pseudonym, code, or number (compare with a writer’s pen name). This is referred to as pseudo-anonymity. It is used frequently in the “witness protection” program. This is the most common variant of anonymity.

- Untraceable identity: One is not known by any name including pseudo-names.

- Anonymity with a pseudo-address to receive and send correspondence with others: This technique is popular with people using anonymous remailers, user groups, and news groups.

Anonymity and the Internet

The nature of the Internet, with its lack of political, cultural, religious, and judicial boundaries, has created a fertile ground for all faceless people to come out in the open. In particular, the Internet provides two channels through which anonymous acts can be carried out:

1. *Anonymous servers:* With advances in software and hardware, anonymity on the Internet has grown through anonymous servers.

   There are two types of anonymity servers:

   a) Full anonymity servers, where no identifying information is forwarded in packet headers.
   b) Pseudonymous servers, which put pseudonym in forwarded packet headers, keeping the real identity behind a pseudonym, but being able to receive and forward all packets sent to the pseudonym to the real server. (Anonymity servers are able to accomplish this through the use of encryption.

2. *Anonymous users:* Another Internet channel to assure anonymity is for users to assume pseudonyms and use internet services such as bulletin boards, chat rooms, and social online networks anonymously. Sensitive and sometimes highly personal or classified information has been posted to popular user groups, news groups, online social networks, and chat rooms. Anonymity of postings is also assured through the use of data transmission protocols such as Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP), which accept messages to servers with arbitrary field information.

Anonymity on the Internet, both anonymity and pseudonymity are not 100% anonymous. As anybody with a rudimentary knowledge of computing networking would know, there is always a possibility to find those who misuse the Internet this way.

Advantages and Disadvantages of Anonymity

There are several advantages to anonymity

- Anonymity is good when a whistle-blower uses it to check unhealthy activities within the organization. Although whistle-blowers are controversial, they are good in a number of cases, especially when there is abuse of office and resources.
- Anonymity is good in case of national security. So underground spies can gather information that is good for national defense.
- Where there is intimidation and fear of reprisals, anonymity is good because useful information may be revealed.
- Anonymity is good for some relationships and the security of some people.

There are also disadvantages to anonymity including:

- Criminals and embezzlers can use it to their advantage, especially in online social networks.
- Lots of disputes could be solved if information from individual's party to these disputes can reveal the necessary information.

2. Security (Vallejos, Mentac, Mayoya, Gopez)

In general, security can be considered a means to prevent unauthorized access, use, alteration, and theft or physical damage to property.

Three elements:

1. *Confidentiality:* To prevent unauthorized disclosure of information to third parties. This is important in a number of areas including the disclosure of personal information such as medical, financial, academic, and criminal records.

2. *Integrity:* To prevent unauthorized modification of files and maintain the status quo. It includes system, information, and personnel integrity. The alteration of information may be caused by a desire for personal gain or a need for revenge.

3. *Availability*: To prevent unauthorized withholding of information from those who need it when they need it. We discuss two types of security: physical security, which involves the prevention of access to physical facilitates like computer systems, and information security, which involves prevention of access to information by encryption, authentication, and other means.

Physical Security

A facility is physically secure if it is surrounded by a barrier such as a fence, has secure areas both inside and outside the facility, and can resist penetration by intruders. Physical security can be guaranteed if the following four mechanisms are in place: deterrence, prevention, detection, and response.

1. *Deterrenc*e to try to defend systems against intruders who may try to gain access. It works by creating an atmosphere intended to scare intruders.

2. *Prevention* used in mechanisms that work by trying to stop intruders from gaining access.

3. *Detection* should be the third line of defense. This mechanism assumes the intruder has succeeded or is in the process of gaining access to the system. So it tries to "see" that intruder who has gained or who is trying to gain access.

4. *Response* is an aftereffect mechanism that tries to respond to the failure of the first three mechanisms. It works by trying to stop and/or prevent damage or access to a facility.

Physical Access Controls

To ensure physical security, a regime of access controls must be put in place. In physical access control, we create both physical barriers and electronic protocols that will authenticate the user of the resource whose security we are safeguarding.

Physical Security Barriers

The physical barrier can be anything that will hinder access to a protected resource including fences, brick walls, mounted motion detection sensors, security lighting, closed-circuit television (CCTV), buried seismic sensors, or different photoelectric and microwave systems. The area surrounding the facility can be secured using locks and keys, window breakage detectors, infrared and ultrasonic detectors, interior microwave systems, animal like dogs, and human barriers like security guards and others.

Electronic Access Controls

With advances in technology, we are moving away, though not totally, from the physical barriers to more invasive electronic controls that include card access control systems and firewalls, and the third and probably the most important area, the inside, may be secured using electronic barriers such as firewalls and passwords.

Passwords

A password is a string of usually six or more to verify a user to an information system facility, usually digital system. Password security greatly depends on the password owner observing all of these four "never" cardinal rules:

1. Never publicize a password.
2. Never write a password down anywhere.
3. Never choose a password that is easy to guess.
4. Never keep the same password for an extended period of time.

Password security is not only important to individuals whose files are stored on a system but it is also vital to the system as a whole because once an intruder gains access to one password; he or she has gained access to the whole system, making all its files vulnerable. So system security is the responsibility of every individual user of the system.

Firewalls

A firewall is hardware or software used to isolate the sensitive portions of an information system facility from the outside world and limit the potential damage that can be done by a malicious intruder. Although there is no standardization in the structure of firewalls, the choice of firewalls depends on the system manager's anticipated threats to the system.

Most firewalls are variations of the following three models:

- *Packet filters:* These are packet-level filters. They contain gates that allow packets to pass through if they satisfy a minimum set of conditions and choke or prevent those packets that do not meet the entry conditions. The minimum conditions may include packets to have permissible origin or destination addresses, as determined by the network administrator. The filter firewalls can also configure and block packets with specific TCP or UDP packet port numbers, or filter based on IP protocol types.

- *Proxy servers:* Work on the protected portions of the network that usually provide information to outside users requesting access to those portions. That is, the firewall protects client computers from direct access to the Internet. Clients direct their requests for an Internet connection through the proxy server. If individual client requests conform to the preset conditions, then the firewall will act on the request; otherwise, it is dropped. These firewalls require specialized client and server configuration depending on the application.

- *Stateful inspection:* These firewalls combine both the filter and proxy functions. Because of this, it is considered complex and more advanced. The conditions for a stateful inspection are, like the filter, based on a set of rules. But unlike filters, these rules are not based on TCP or UDP but on applications like proxy servers. They filter packets by comparing their data with archived friendly packets.

Information Security Controls

Information security includes the integrity, confidentiality, and availability of information at the servers, including information in files and databases and in transition between servers and between clients and servers. The security of information can be ensured in a number of ways. The most common are cryptography for information transmission and authentication and audit trails at the information source and information destination servers.

Cryptography, the science of writing and reading coded messages, forms the basis for all secure transmission. This is done through three functions: symmetric encryption, asymmetric encryption, and hash functions.

Encryption

Encryption is a method that protects the communications channel from sniffers—programs written for and installed on the communication channels to eavesdrop on network traffic, examining all traffic on selected network segments.

Sniffers are easy to write and install and difficult to detect. Cryptography uses an encryption algorithm and key to transform data at the source, called plaintext; turn it into an encrypted form called ciphertext, usually an unintelligible form; and finally recover it at the sink.

The encryption algorithm can be either symmetric or asymmetric.

Symmetric encryption, or secret-key encryption as it is usually called, uses a common key and the same cryptographic algorithm to scramble and unscramble the message as shown in Fig. 5.1.

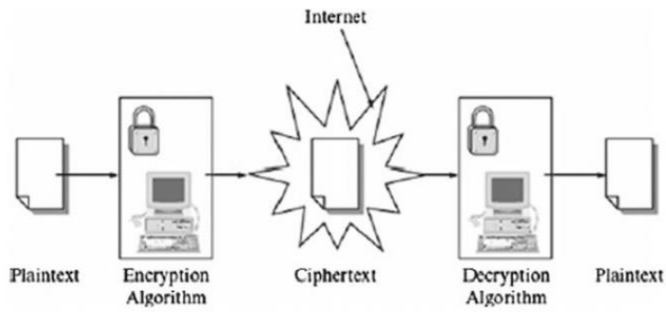

Fig. 5.1 Symmetric encryption

One problem with symmetric encryption is the security of the keys which must be passed from the sender to the receiver.

Asymmetric encryption, commonly known as public-key encryption, uses two different keys, a public key known by all and a private key known by only the sender and the receiver. Both the sender and the receiver each have a pair of these keys, one public and one private. To encrypt a message, from sender A to receiver B, as shown in Fig. 5.2, both A and B must create their own pairs of keys. Then, A and B exchange their public keys—anybody can acquire them. When A is to send a message M to B, A uses B's public key to encrypt M. On receipt of M, B then uses his or her private key to decrypt the message M.

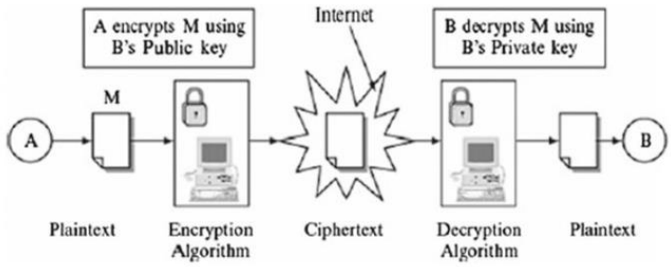

Fig. 5.2 Asymmetric encryption

A **hash** function takes an input message M and creates a code from it. The code commonly referred to as a hash or a message digest will be discussed more in the next section. A one-way hash function is used to create a digital signature of the message—just like a human fingerprint. The hash function is therefore used to provide the message's integrity and authenticity.

Authentication

Usually, it is difficult for a system to verify the identity of a user, especially a remote user. Thus, authentication is a process, whereby the system gathers and builds up information about the user to assure that the user is genuine.

In **data communication**, authentication is also used to ensure the digital message recipient of the identity of the sender and the integrity of the message.

In **computer systems**, authentication protocols based on cryptography use either secret-key or public-key schemes to create an encrypted message digest that is appended to a document as a digital signature.

The **digital signature** is similar to a handwritten signature in printed documents. Just like handwritten signatures, digital signatures ensure that the person whose signature the system is authenticating is indeed the true person, but digital signatures provide a greater degree of security than handwritten signatures.

Also, digital signatures once submitted can never be disowned by the signer of a document claiming the signature was forged. This is called nonrepudiation.

A secure digital signature system consists of two parts:

(1) a method of signing a document and

(2) authentication that the signature was actually generated by whoever it represents

Physical Authentication Methods.

Authentication of users or user surrogates is usually based on checking one or more of the following user items:

- Username (sometimes screen name).
- Password.
- Biometrics like retinal images: The user looks into an electronic device that maps his or her retinal image; the system then compares this map with a similar map stored on the system.

- Fingerprints: The user presses on or sometimes inserts a particular finger into a device that makes a copy of the user fingerprint and then compares it with a similar image on the system user file.

- Physical location: The physical location of the system initiating an entry request is checked to ensure that a request is actually originating from a known and authorized client machine. To check the authenticity of such a client, the network or Internet Protocol (IP) address of the client machine is compared the one on the system user file. This method is used mostly in addition to other security measures because it alone cannot guarantee security: If used alone, it provides access to the requested system to anybody who has access to the client machine.

- Identity cards: Increasingly, cards are being used as authenticating documents. Whoever is the carrier of the card gains access to the requested system. As is the case with physical location authentication, card authentication is usually used as a second-level authentication tool because whoever has access to the card automatically can gain access to the requested system.

Operational Security

Operation security involves policies and guidelines that organizations including all employees must do to safeguard the assets of the organization including its workers. These policy guidelines are spelt out in a document we call a security policy. It also includes guidelines for security recovery and response in case of a security incident.

3. Privacy (Nepa, Nolasco, Collantes, Gaspar)

Privacy is a human attribute consisting of four elements of solitude, anonymity, intimacy, and reserve. Each one of us possesses these elements as rights.

We put these rights into two categories.

The **first category** includes three rights that an individual can use to fence off personal information seekers.

1. **Control of external influences:**
   - *Solitude*: The right to be alone without disturbances
   - *Anonymity*: The right to have no public personal identity
   - *Intimacy*: The right not to be monitored.

The **second category** contains those rights an individual can use to control the amount and value of personal information given out.

2. **Control of personal information:**
   - *Reserve:* The right to control one's personal information including the methods of dissemination of that information.

The notion of privacy is difficult to accurately define because the definition of privacy depends on things like culture, geographical location, political systems, religious beliefs, and a lot more.

Types of Privacy

1. *Personal Privacy*

   This type of privacy involves the privacy of personal attributes. The right to privacy of all personal attributes would mean the prevention of anyone or anything that would intrude or violate that personal space where those attributes are. This would include all types of intrusions including physical searches, video recording, and surveillance of any type.

2. *Informational Privacy*

   Informational privacy, unlike personal privacy, concerns the protection of unauthorized access to information itself.

   Of course there are different strands of information that we have to protect including:

   - **Personal information:** Most personal information of value includes information on personal lifestyles like religion, sexual orientation, political affiliations, or personal activities.

   - **Financial information:** Financial information is important not only to individuals but also to organizations. Financial information is a very valued asset because it gives the organization the autonomy it needs to compete in the market place.

   - **Medical information:** Medical information is very personal and very important to all of us. For personal, employment, and insurance purposes, many people want their medical information to be private.

   - **Internet:** In this new age, the Internet keeps track of all our activities online. With an increasing number of people spending an increasing number of time online in social networks and the digital convergence becoming a reality with every passing day, not only will our social life be online but soon all our lives also will.

3. *Institutional Privacy*

   Institutions and organizations want their data private not only for business advantages but also for the life of the business. The research data, the sales and product data, the marketing strategies, and the activities of the organization all need to be private.

Value of Privacy

Privacy has traditionally been perceived as valuable and has even gained more importance in the information age because it guards an individual's personal identity, preserves individual autonomy, and makes social relationships possible.

<u>Three attributes of privacy</u>

1. *Personal Identity*

   Personal identity is valuable because it enshrines personal privacy.

2. *Autonomy*

   Humans need to feel that they are in control of their own destiny. They need their autonomy. The less personal information people have about an individual, the more autonomous that individual can be, especially in decision making. However, other people will challenge one's autonomy depending on the quantity, quality, and value of information they have about that individual. People usually tend to establish relationships and associations with individuals and groups that will respect their personal autonomy, especially in decision making.

3. *Social Relationships*

   In some societies where marriages are arranged, parents on both sides try to collect as much information about each other as possible before they commit their offspring in marriage. In societies where there are no arranged marriages, the parties involved usually spend a period of time dating. The dating time is spent collecting as much information as possible about each other. The couple then uses this information to make a decision about marrying. However, each party may try to conceal some information because some seemingly valuable information may not be worthwhile and may even lead to breakup of the relationship.

Privacy Implications of Database System

Information Gathering

The information they collect from us is put into databases and is later sold to the highest bidder, usually a marketer.

Information gathering is a very serious business that is increasingly involving a growing number of players that traditionally governments gathering mostly defensive information on weapon systems. However, with globalization and the Internet, the doors to the information gathering field have been cast open. Now, individuals, companies and organization, and of course governments are all competing, sometimes for the same information.

With the modern tools of gathering information, no one is safe anymore. Because of our habits online, Internet crawlers are in action visiting our machines stealthy and gathering a wealth of information. There is no longer the need to get your information from cards you fill at shopping malls and grocery stores. There are better and faster ways now. There are tremendous legal and privacy issues that we have to deal with. First, most of the information collected from us, the one we come to know of, which is a fraction of what they take, is collected without our consent.

Privacy Violations and Legal Implications

There are numerous contributing factors or causes of violations.

1. Consumers willingly give up information about themselves when they register at Web sites, shopping malls in order to win prizes, and in mailing solicitations.
2. Consumers lack the knowledge of how what they consider a little bit of information can turn into a big invasion of privacy.
3. Inadequate privacy policies.

4. Failure of companies and institutions to follow their own privacy policies. 5. Internet temptation, that enables businesses to reach individuals in a very short time in the privacy of their homes and offices.

Other privacy violations include **intrusion, misuse of information, interception of information, and information matching.**

Intrusion

Intrusion is an invasion of privacy by wrongful entry, seizing, or acquiring possession of the property of others. For example, hackers are intruders because they wrongfully break into computer systems whether they cause damage or not. With computer network globalization, intrusion is only second to viruses among computer crimes, and it is growing fast.

Misuse of Information

There is nothing wrong with collecting personal information when it is going to be used for a legitimate reason, for the purpose it was intended. However, the problem arises when this information is used for unauthorized purposes; collecting this information then becomes an invasion of privacy.

Interception of Information

Interception of information is unauthorized access to private information via eavesdropping, which occurs when a third party gains unauthorized access to a private communication between two or more parties. Information can be gathered by eavesdropping in the following areas:

- At the source and sink of information, where either client or server intrusion software can listen in, collect information, and send it back to the sender
- Between communication channels by tapping into the communication channels and then listening in.

Information Matching

The danger with information matching is that there is no limit to what one can do with the collected information, and no one knows what the profiles built from the matched information will be used for and by whom. Hundreds, maybe thousands, of databases with individual records are gathered from an individual over a lifetime.

The threat to information matching does not only originate from linking individual records in different databases. It also can come from erroneous or outdated (stale) information.

Errors can enter information in basically three areas:

1) at the source, where it occurs mainly through incorrect input such as typing the letter “l” of the alphabet instead of a “1” (one);
2) during transmission because of transmission interference; and
3) at the sink, mainly as a result of poor reception. Information becomes stale when it gets outdated. Unfortunately, erroneous and stale information is frequently used.

Privacy Protection and Civil Liberties

Many rights scholars have different sets of rights that they put under the umbrella of civil liberties.

But the most accepted set of civil liberties is grouped into the following four categories:

1) criminal justice that includes police powers, personal liberty, and the right to a fair trial;
2) basic freedoms of speech, assembly, association, movement, and no discrimination;
3) freedom of information; and
4) communications and privacy.

Personal privacy is a basic civil liberty that must be protected like any other civil liberty such as the right to free speech. In many countries, there are guidelines and structures that safeguarded and protected privacy rights.

These structures and guidelines, on the average, fall under the following categories:

1. **Technical**: Through the use of software and other technically based safeguards and also by education of users and consumers to carry out self-regulation. For example, the Electronic Frontier Foundation has the following guidelines for online safeguards:

    a) Do not reveal personal information inadvertently.
    b) Turn on cookie notices in your Web browser, and/or use cookie management software or infomediaries.
    c) Keep a “clean” email address.
    d) Don’t reveal personal details to strangers or just-met “friends.”
    e) Realize you may be monitored at work. Avoid sending highly personal emails to mailing lists, and keep sensitive files on your home computer.
    f) Beware of sites that offer some sort of reward or prize in exchange for your contact or other information.
    g) Do not reply to spammers, for any reason.
    h) Be conscious of Web security.
    i) Be conscious of home computer security.
    j) Examine privacy policies and seals.
    k) Remember that you alone decide what information about yourself to reveal — when, why, and to whom.
    l) Use encryption

2. **Contractual**: Through determination of which information such as electronic publication, and how such information is disseminated, is given contractual and technological protection against unauthorized reproduction or distribution. Contractual protection of information, mostly special information like publications, is good only if actions are taken to assure contract enforceability.

3. **Legal:** Through the enactment of laws by national legislatures and enforcement of such laws by the law enforcement agencies.

Philippine Legislation on data privacy

DATA PRIVACY ACT (RA 10173)

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

RA 10173 regulates the processing of personal information of individuals collected by both public and private entities as a way to protect one's privacy.

Under this act, an individual shall be given the right to control any kind of personal information that is collected from him for further use and disclosure.

Under Section 11 of the data privacy law, personal information must be:

a. Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

b. Processed fairly and lawfully;

c. Accurate, relevant and where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed, or their further processing restricted;

d. Adequate and not excessive in relation to the purposes for which they are collected and processed;

e. Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or provided by law; and

f. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, that personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, that adequate safeguards are guaranteed by said laws authorizing their processing.

VI. LEARNING ACTIVITIES

General Rules: 1. Downloaded answers from the Internet will not be considered.
2. Copied answers from your classmates either from BSCS, BSInte 4A and BSInte 4B will be nullified for all students with the same answers.

Scenario: (Source: https://www.pna.gov.ph/articles/1118282)

With the present pandemic, contact tracing has been a primary response in addressing the coronavirus disease 2019 (COVID-19). Customers or clients of a certain organization are required to fill-up forms upon entering their establishment as a form of contact tracing.

However, the National Privacy Commission (NPC) announced that it was looking into reports on the misuse and mishandling of data retrieved by some business establishments from contact tracing efforts.

The NPC, in a statement, said customers raised concerns over “the improper use of logbooks and the lack of appropriate data-protection measures that left in the open filled-out contact-tracing forms that contain customers’ data, such as names, addresses and contact details, which other people could see."

Other concerns were that “personal data were used for purposes other than contact tracing in the absence of a privacy notice and baseless retention period,” the agency said.

"We hear out the sentiment of the public and their encounters with establishments that violate privacy rights and employ inappropriate security measures," NPC Commissioner Raymund Liboro said.

Discussion Questions:

1. Do you believe we still have individual privacy?
2. What do you think is the best way to safeguard privacy?
3. How much interference by government in your life can you tolerate in order to feel secure?
4. How much privacy are you willing to give up to feel secure?

VII. EVALUATION

To be scheduled

VIII. ASSIGNMENT

IX. REFERENCES

a. Book/Printed Resources

Laviña, Charlemagne G. (2015). Social, Ethical, Legal and Professional Issues in Computing. Mindshapers Co., Inc.

b. e-Resources

Adams, M. (n.d.). *Security vs. Privacy vs. Anonymity: Understanding the Differences*. BusinessTechWeekly.com. Retrieved October 28, 2021, from https://www.businesstechweekly.com/cybersecurity/data-security/security-privacy/.

Kizza, Joseph Migga (2017). Ethical and Social Issues in the Information Age (6th ed.) [eBook Edition]. Springer International Publishing. https://www.pdfdrive.co

Ot, A. (2021, March 20). *Privacy vs. anonymity vs. security: Why they don't all mean the same thing*. MUO. Retrieved October 28, 2021, from https://www.makeuseof.com/privacy-anonymity-security-mean/.

link.springer.com.(n.d.). *Anonymity, security, and privacy*. Retrieved October 28, 2021, from https://link.springer.com/chapter/10.1007%2F978-1-4757-2950-4_4.

www.cs.unh.edu (n.d.). *Privacy, Anonymity, and Data Gathering*. Retrieved October 28, 2021, from https://www.cs.unh.edu/~sna4/cs408/Text/Section0003.xhtml.