UNIVERSITY OF WESTMINSTER

INFORMATICS INSTITUTE OF TECHNOLOGY

Trends in Computer Science

Module: 4COS008C

CYBER SECURITY

What is Computer Ethics?

What are the ethical implications of collecting data about users?

Abhinav Ratnathurai

w1904573

20211507

Group D (1) Members-

20211507	Abhinav Ratnathurai (Team Leader)
20211360	Vinuk Senadeera
20210563	Mahen Abeykoon
20211508	Ravindu Ariyarathne

ACKNOWLEDGMENT

I would like to acknowledge and give my warmest thanks to Ms. Sulochana Rupasinghe who made this work possible. Her guidance during lectures and the advice she gave, carried me through all the stages of writing my project. I would also like to thank my Team members for letting my defense be an enjoyable moment, and for your brilliant comments and suggestions, thanks to you.

ABSTRACT

As the public becomes increasingly computer literate, the gap between technology and peoples' mental power notably shrinks. The available computer resources, software, and assorted output devices have enlightened many unethical activities, privacy invasion, and illegal purposes. Academic scholars and industry practitioners consider computer ethics to be one of the most important topics of concern and interest. They are described as an all-encompassing word that refers to all efforts required to safeguard information and systems supporting ethical usage. When collecting data about users there are several rules and regulations. The users must be told who can see their details and other details on what happens to their data which we collect from them. We can see how cyber laws connect with the ethical implications of collecting data about users. Cyber laws are normally created after a problem occurs because there are cyber laws that were created after a problem caused due to hacking of users' data.

Keywords

Computer ethics, collecting data about users, Cyber laws against stealing users' collected data, and Implications when collecting data.

TABLE OF CONTENTS BOOKMARK

LIST OF FIGURES

CHAPTER 1--INTRODUCTION

The use of computers is controlled by a set of standards of right and wrong known as computer ethics. New cyber threats emerge continuously, and a successful company must do all possible to stay ahead of the competition. In the world of computer security, cyber-ethics differentiates security professionals from hackers. (Alan Calder, 2020). The goal of ethics is to help us agree on how we will live and work together, not to judge us.(John Hooker, 2018)

CHAPTER 2-COMPUTER ETHICS

Individual ethical aids in the identification and distinction of right-thinking, judgments, and acts from those that are incorrect, hurtful, and/or destructive to others and oneself. Values, ideas, emotions, and sentiments, as well as facts, inform and drive ethical behavior.

CRITERIA IN ETHICAL REASONING:

1. Set customs must follow a logical pattern. The assumptions and premises utilized to create judgments, both genuine and deduced, must be known, and made plain.

2. The facts used to support a person's decision should be correct, relevant, and complete.

3. When thinking, ethical norms should be consistent. When contradictions in a person's ethical standards are revealed during a choice, one or more of the criteria must be changed. **(Joesph W.Weiss, 2021)**

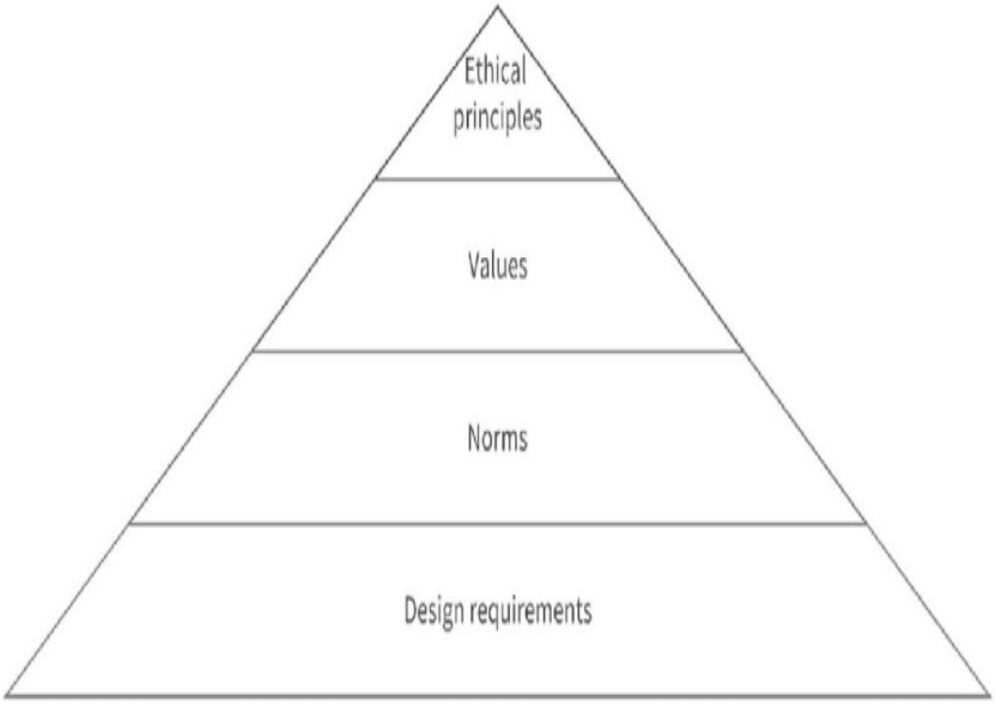

Figure 1 Computer Ethics.

CHAPTER 3-THE ETHICAL IMPLICATION WHEN COLLECTING DATA ABOUT USERS. Figure 1 Computer Ethics

The gathering of data is a critical component of community health improvement activities. Surveys, interviews, and observation are used to collect the bulk of data. There are many things to keep in mind when collecting data, here are a few of them:

3(I). DON'T PROMISE TO SHARE DATA.

Too frequently, consent forms guarantee that users' data will be kept "private and secret to the degree authorized by law," or that "only the study team will have access" to it. Such unthinking assurances are frequently included in current permission forms based on previous studies. Users may submit consent forms that claim the data will not be disclosed or regarding data sharing. If the user subsequently decides to or (due to developing journal and sponsor regulations) must disclose data, this topic technique will pose significant complications.

3(II) DO GET CONSENT RETAIN TO AND SHARE DATA.

Users should be aware of who will have access to their data. Users can choose from a variety of permission choices to give them some control over how their data is used for secondary research. There are two options: That is, users can be given the option of sharing some but not all of their data, as well as sharing their data with some but not all groups. Yet, if users' sole option is to consent to their data being shared as indicated in the protocol or not to participate in the research at all, it will typically be ethically acceptable.

3(III) Sharing Data That Were Previously Collected Without Explicit Consent to Share:

Data sharing poses two risks to participants. One risk is that their data will be associated with their identity by someone they did not choose to share that identified data with; this can lead to harm, in addition to the basic loss of privacy. The other concern is that users' data, even if it isn't linked to their identities, will be used for research for which they haven't given their approval, making them complicit in what they consider to be inappropriate study. (Michelle N. Meyer, 2018)

CHAPTER 4 - CYBERLAW.

Cyber law is the branch of law concerned with the link of the Internet to technological and electronic aspects such as computers, software, hardware, and information systems (IS). So many of today's cyber laws are reactive, meaning that something happened, and then a law was created to try to prevent it from occurring again. These laws are used to protect users, organizations, and companies from their collected data being hacked or stolen by hackers. When Yahoo suffered its first major data breach in **2016**, hackers stole about 500 million **accounts** dating back to **2014.** The necessity for data protection was inspired by this incident, and the **Consumer Privacy Protection Act** of **2017** was passed as a result. Here's a quick rundown of current cyber regulations which are more likely to hear:

- The **1996** Health Insurance Portability and Accountability Act (HIPPA) was **enacted to safeguard individual health records.**
- The **2017 Consumer Privacy Protection Act** (CPPA): This rule was **enacted immediately after the massive Yahoo data breach in 2016, to protect consumer information and prevent identity theft.**
- The General Data Protection Regulation (GDPR) of **2018** is the strictest privacy and security regulation in the world, and it influences US activities.
- The **2018** California Consumer Privacy Act (CCPA): This was the first statute approved in the United States to **defend consumers' rights by allowing them more choice over how their personal information is shared**.

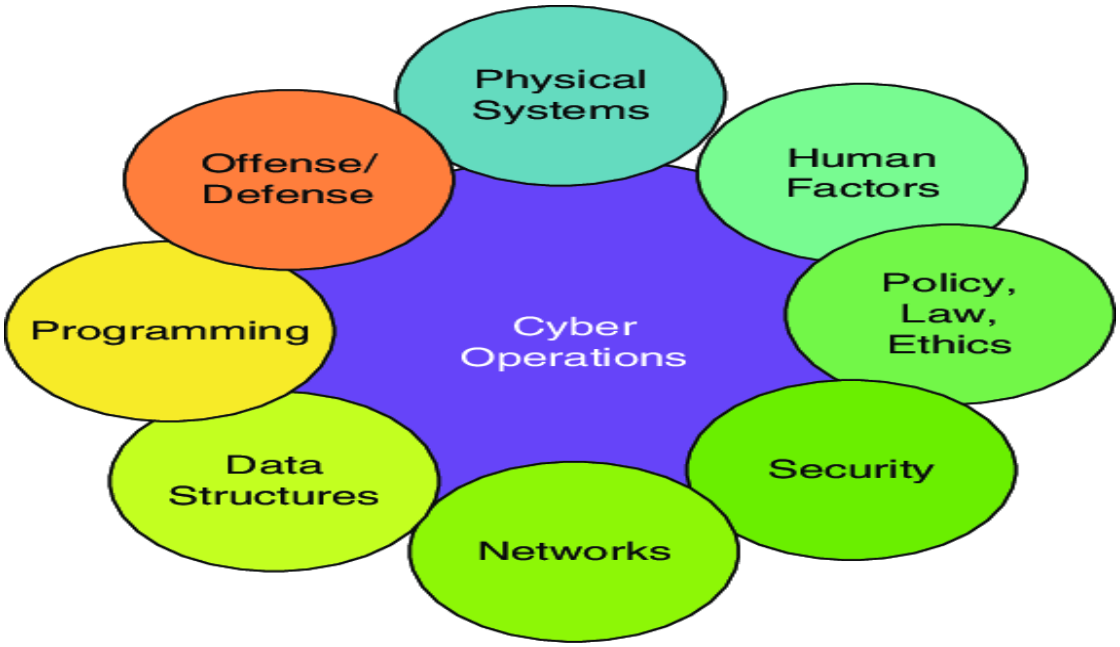

Figure 2: Cyber Operations

CHAPTER 5-CRITICAL EVALUATION

Information security requires (CIA) Integrity, Confidentiality, and Availability to secure the data collected about users without losing all those data. Below are some fundamental things to remember when collecting data:

- Personal data collection and usage should be confined to certain objectives.
- To minimize unnecessary data collection and "function creep," both of which can pose privacy problems, the data acquired must be appropriate to the goal**.**
- **Personal data should only be collected and used on legal grounds**, etc.

Dr. Gerald Auger, Jaclyn Jax Scott, Jonathan Helmus, Kim Nguyen, and Heath the Cyber Mentor Adams, 2020)

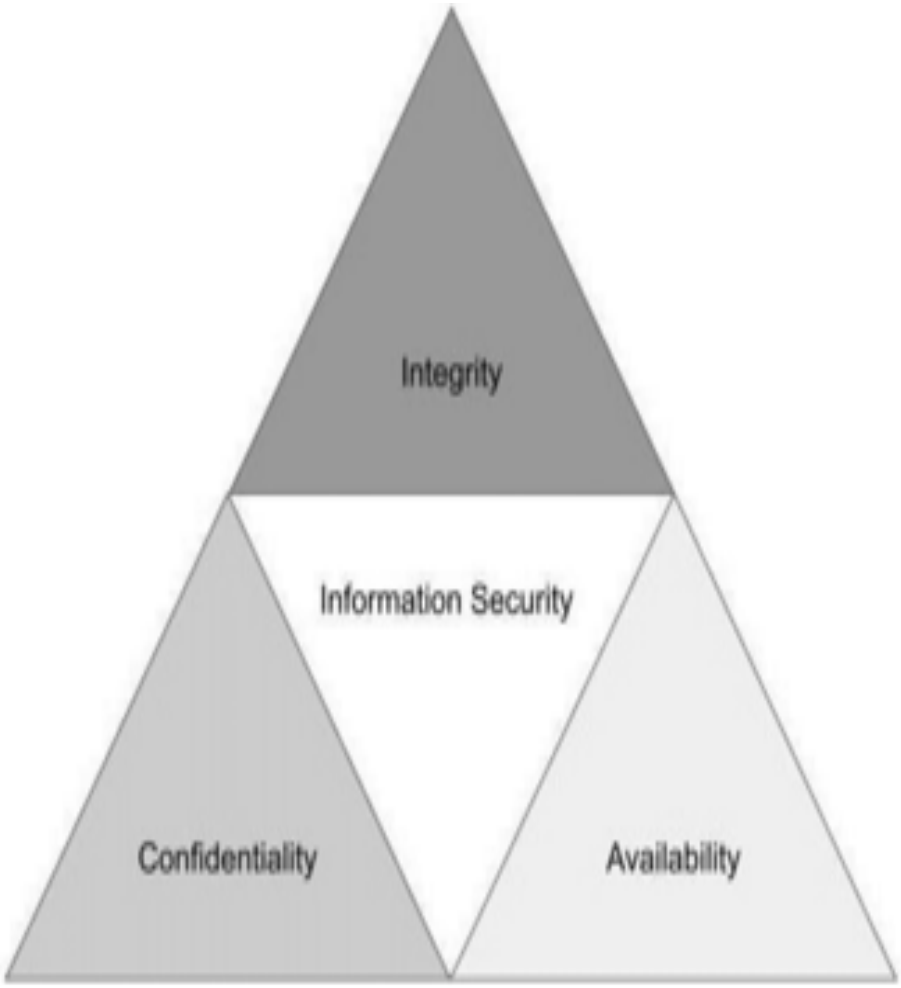

Figure 3: CIA Triad

CHAPTER 6-CONCLUSION

By collecting data, you can maintain and review crucial information about your existing and potential customers. By compiling this data, the organization may save money by creating a consumer database for future marketing and retargeting initiatives. Surveillance systems may be effective regardless of the data type or how it is gathered provided the implementers and end-users understand the data's and collection methodology's limitations and incorporate that information into their interpretation methods.

References:

Alan Calder. (2020). Cyber security, Essential Principles to Secure Your Organisation, IT Governance Publishing (ITGP), Available from https://learning.oreilly.com/library/view/cyber-security-essential/9781787782112/, [Accessed 14th.July.2022]

Gabby Hibberd. (2022). The Art of Cyber Security. IT Governance Publishing (ITGP). Available from https://learning.oreilly.com/library/view/the-art-of/9781787783676/ . [Accessed 14.06.2022]

Dr. Gerald Auger, et al. (2020). Cybersecurity Career Master Plan. Livery Place 35 Livery Street Birmingham B3 2PB, UK. Packt Publishing. Available from https://learning.oreilly.com/library/view/cybersecurity-career-master/9781801073561/. [Accessed 16.06.2022]

John Hooker. (2018). Talking Ethics Seriously. New York, New York, United States. Productivity Press. Available from https://learning.oreilly.com/library/view/taking-ethics-seriously/9781351578677/. [Accessed 15.06.2022]

Joseph W. Weiss. (2021). Business Ethics, Seventh Edition. 1333 Broadway #1000, Oakland, CA 94612, United States. Berrett-Koehler Publishers. Available from https://learning.oreilly.com/library/view/business-ethics-seventh/9781523091560/. [Accessed 18.06.2022]

LOZOVANU, Ecaterina. (2019). Computer ethics – problems and solutions. Technical University of Moldova, 168, Ștefan cel Mare Blvd. Chișinău, Republic of Moldova. Universitatea Tehnică a Moldovei. Available from http://cris.utm.md/bitstream/5014/403/1/86-86_11.pdf . [Accessed 15.06.2022]

Meyer, M. N. (2018) 'Practical Tips for Ethical Data Sharing', Advances in Methods and Practices in Psychological Science, pp. 131–144. DOI: 10.1177/2515245917747656.

Figure 1: Cawthorne, Dylan & Wynsberghe, Aimee. (2020). An Ethical Framework for the Design, Development, Implementation, and Assessment of Drones Used in Public Healthcare. Science and Engineering Ethics. 26. 10.1007/s11948-020-00233-1.

Figure 2: Ivy, Jessica & Lee, Sarah & Franz, Dana & Crumpton, Joseph. (2019). Seeding Cybersecurity Workforce Pathways With Secondary Education. Computer. 52. 67-75. 10.1109/MC.2018.2884671.

Figure 3: Dr. Gerald Auger, et al. (2020). Cybersecurity Career Master Plan. Livery Place 35 Livery Street Birmingham B3 2PB, UK. Packt Publishing. Available from https://learning.oreilly.com/library/view/cybersecurity-career-master/9781801073561/ . [Accessed 16.06.2022]