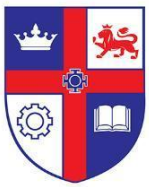
LONDON METROPOLITAN UNIVERSITY



islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5052NI Professional Issues Ethics and Computer Law

Assessment Weightage & Type

60% Individual Coursework

Year and Semester

2022-23 Spring

Student Name: Niwesh Dhital

London Met ID: 21049549

College ID: np01cp4a210205

Assignment Due Date: Monday, May 1, 2023

Assignment Submission Date: Monday, May 1, 2023

Word Count: 3502

I confirm that I understand my coursework needs to be submitted online via MySecondTeacher under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Content

Table of Figures

1) Introduction

LinkedIn is a massive social media platform where job seekers as well as job providers can communicate on common ground and make connections concerned with their profession (Hanna, 2022). Professionals provide their resumes and share their work experience to attract attention and get a job, potentially. Reid Hoffman, Allen Blue, Konstantin Guericke, Eric Ly, and Jean-Luc Vaillant founded LinkedIn (Gregersen, 2022). Naturally, privacy should be of major concern for a company of such scale. However, this could not be farther from the truth.

Privacy and data security are legitimate issues in the digital age where millions of individuals are on the internet, daily. So, governments all over the world should be able to protect their citizens from unprecedented cyber-attacks and so, there are various countries across the world that have laws in place to do the exact same. LinkedIn is one of many companies on the internet that collaborates with people and works with their data and to whom the various regulatory measures are applicable. LinkedIn acquired a million users by the end of 2004 and off of the success of the social media site, they introduced premium subscription services that allowed users to access other services besides their standard experience. In 2007, they started working on an expansion of the site's search capabilities and in 2009 they launched the now infamous job feature that allowed users to seek and provide job opportunities through the platform (Reynolds, 2022). In 2023, due to their expansion prowess and proficient business and marketing, the user base of LinkedIn has reached a whopping 875 million people constituting professionals from every field imaginable. Such a mega corporation should have various measures and counter measures in the case of any external threat. Not only that, but such a mega corporation should also put privacy on top of their list of concerns and while many companies claim to have excellent counter measures against cyber-attacks, they tend to fall short when it comes to sticking with their promises and often fall short when it comes to taking accountability after such an issue. Unfortunately, the subject of the report is based on one of such shortcomings and in particular, the LinkedIn data breach that occurred in 2021 that went under the noses of a majority of the people and the mainstream media.

The case of LinkedIn is quite out of the ordinary in a sense that such a huge scandal did not affect the company as much and in fact their customers had no idea of the breach.

2) Background

The data breach scandal was first brought to the public eye in June of 2021 when an online research center named Restore Privacy published a report about the situation (Taylor, 2021). Despite this, the company still failed to properly report on the incident properly and so the far-reaching effects that this could have on their customers is still little known.

The perpetrator was a hacker by the username “TomLiner” who sold the data of their users for 5000 dollars (Nicko,John,Chester , 2023) .They advertised data from seven hundred million people on a hacking forum and claimed to have scraped data by exploiting the Linked API to harvest information of the people embedded with the system (Taylor, 2021). A sample was acquired and evaluated by Restore Privacy via telegram and it was found that in the sample, there were sensitive information such as email addresses, full names, physical addresses, geolocation record and other disconcerting pieces of information that could have been misused by ill-intentioned people (Taylor, 2021). In a statement that LinkedIn later published on their website, the company claimed that the data breach situation was not as dire as people were suspecting and in fact, no private LinkedIn member data was exposed (LinkedIn Corporation, 2021). Prior to the data leak scandal of 2021, LinkedIn had a similar scare back in June of 2012 when the data of 6.5 million people was put in a precarious position and was exploited by hackers (Thorsheim, 2016). However, the incident of 2021 was much grander in scale and exposed almost seven hundred million people’s data to vulnerabilities on the internet when a hacker put the people’s data up for sale on the internet. Initially, the news was disclosed to the public by ‘privacyrestore.com’ who reported that the data of about a million users were put up on telegram, a communication application, and included sensitive information related to their users (Taylor, 2021). Despite this, the company has yet to take proper accountability for their deficiencies. The incident was scarcely reported on and so many of LinkedIn’s customers are still unaware of the particular situation. However, something that could be said for certain is the fact that companies have a way of cleverly masking such situations and making the severity of the situation to be much less severe than it actually is.

The scandal brought in light the jarring deficiencies of a mega corporation where an insignificant source shined a negative light on the company and tampered with the public reputation of the company.

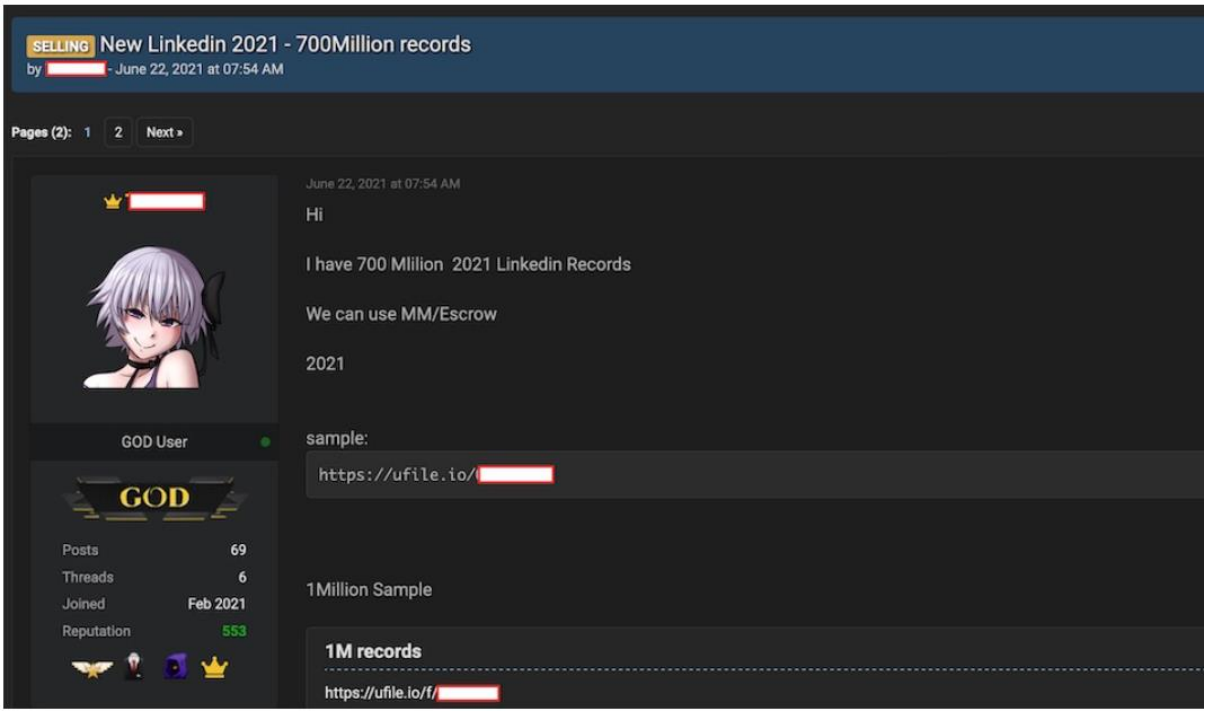


Figure 1: LinkedIn data breach Perpetrator profile and data dump (Taylor, 2021)

Figure 2: Full names, LinkedIn usernames, Facebook usernames, email accounts, mobile phone numbers, professional data, inferred salary, and more (Taylor, 2021).

3) Legal issues

Worldwide, there are several rules and laws protecting users and their data. Linked however, has faced no major judicial outcry until recently, which according to statistics is well within the realm of expectations as only five percent of data breaches have ever ended up leading to class action litigation (Bryan Cave, 2016).

The potential legal ramification that could have been levied upon LinkedIn from an international standpoint are as follows:

- **Government imposed fines**

  In the United Kingdom, not reporting a data breach could lead to a fine of ten million Euros or 2% of an organization's global turnover (Wolford, 2023). And in the case of LinkedIn, though the company was not personally responsible for leaking the information on the internet, they still contributed to the event by making their system susceptible to exploitation from unsavory parties.

- **State punishment in the United States**

  In the United States there is no central law that decides punishment for a data breach but there are certain state rules to incriminate the guilty party in the case of such an event. The state laws are:

  I. The California Consumer Privacy Act (CCPA) of 2018 requires businesses that collect personal information from California residents to supply notice at the point of collection (worldbank.org, 2023). In a data breach as a result of a business's failure to maintain reasonable security procedures and practices, any affected part could sue for the number of monetary damages of up to $750 (oag.ca.gov, 2023). For LinkedIn, this could be applicable as confidential user data was offered to suitors on alternate forums for hefty sums albeit due by an unsavory individual but directly due to the incompetence of LinkedIn.

  II. For New York's Privacy Act that came to effect on January 1st,2020 requires companies to be upfront and transparent in the event of a cyber-attack which allows leeway to the companies in case of judicial predicament (BORNER, 2019). This act levies a fine of up to $5000 per violation and in the event of non-compliance, the maximum penalty rises up to as much as $100,000 (corsica

technologies, 2020). So, in the state of New York, LinkedIn could have been levied an appropriate fine from $5000-$10000 dollars according to the severity of privacy violation, as indicated by the company's hesitance in reporting the situation as it developed.

- **Class action lawsuits**

  Class action lawsuits are filed by a group of people, against a large company in the wake of fraud or other malpractices. Had the issue been widespread in the media, class action lawsuits would have cropped up and LinkedIn would have been looking at payments of substantial amounts of money to all the affected people.

- **Perpetrator specific legal action**

  The perpetrator of the crime which in case of LinkedIn was an unnamed hacker could have faced a lawsuit from the corporation and judicially could have been dealt a hefty sentence and insurmountable fines if brought in front of an international court of justice. For example, in the case of Capital One bank data breach, a software engineer named Paige Thompson was given time served plus five years of probation in 2019 (Faife, 2022).

- **EU specific action against data privacy violation**

  The General Data Protection Regulation (GDPR), one of the world's strictest laws governing privacy and security (Burgess, 2020). A key point of the rule is that a company can be fined if there is a security breach, or it is found that the company is falsely claiming that their system is safe when in fact it might not be (Burgess, 2020). This means that according to the act, a fine of up to 20 million euros or four percent of a firm's global turnover could have been levied upon the company, offsetting a major percentage of their profit (Burgess, 2020).

In the case of LinkedIn, members within the organization could have been subjected to a lengthy trial if taken to court and if found guilty, the high-ranking officials and the people concerned with the event could have been incarcerated as well. In addition to that, the data from LinkedIn could have been implicated as an indirect preparator due to their lack of professional incompetence,

4) Social Issues

There are various social implications that come with privacy invasion. LinkedIn, a company with such a clear and concise brand tempered its standing in the public eye with the data breach. Regardless of the legal situation, there are bound to be social issues that come with such a concerning invasion of privacy.

Some major social impacts of data breach also applicable for the situation of LinkedIn are as follows:

- **Consumer mistrust**

  In the United States in the year 2022 alone, 422 million individuals were affected by data compromises such as data breaches, leakage and exposure that led to sensitive information being leaked for exploitation by unsolicited parties (Petrosyan, 2023). Such jarring deficiencies have taken a considerable toll on customers to the point where 58% of adults are now more than ever worried about being a victim of a cybercrime (Stouffer, 2022). The LinkedIn situation could have played its part in contributing to the hysteria as well.

- **Extensive turmoil**

  Cyberattacks could be an extremely drawn-out process that could disrupt people's lives. In 2019, more than twenty towns sharing a software vendor were targeted by a cyber-attack where the perpetrators asked for a ransom of 2.5 million dollars for the restoration of administrative services. The people were not allowed to access records or pay bills while this was going down (Allyn, 2019). In 2012, when a similar data breach incident occurred in LinkedIn in 2012, the company forced a password reset for an extremely specific subset of their userbase. And there is no say in how the situation is going to turn out in the future.

- **Psychological impact**

  There is no definitive proof of the amount of stress that a data breach causes. However, something that can be said is that an event where the perpetrator gained access and leaked sensitive information out in the public for exploiters could be traumatic for most people out there. Psychologically, having the thought of someone going through one's

personal belongings could be nightmare inducing. In the case of LinkedIn when such a scandal occurred, many people were unaware. But the people who were aware must have been constantly under the presumption that their confidential information was under threat of exploitation.

- **Identity theft**

  Identity theft could be caused by exposing personal information that can have drastic impacts on an individual's life such as monetary loss, low credit score and other things. Identity theft can also cause a lot of self confidence in companies that manage personal data.

- **Social engineering attacks**

  Individuals who gain access to personal information through a data breach may use social engineering attacks to deceive others, potentially leading to further loss of personal information or unauthorized access to confidential systems and data.

Overall, a data breach has adverse effects on the human psyche and in the case of LinkedIn though the incident was not as widespread, the points above could prove to be an indicator of the consequences that such an event could have had on society.

5) Ethical Issues

Ethically, data violation is not something to rave about to say the least. In fact, the ability to not provide services to people who rely on others for the said services directly interfere with certain fundamentals of the code of ethics.

The several ways in which LinkedIn came short are as follows:

- **Rule based Obligation (Deontology)**

  As dictated by the theory of deontology, truthfulness is the primary aspect of practicing ethics. In the example of LinkedIn, the company has repeatedly shown how it can lie. The situation of 2012 data breach of LinkedIn could be a prime example of such a tendency (Thorsheim, 2016). So, to say that the company could have violated the rule again is entirely possible (Baase, 2012).

- **Disregard for natural rights**

  Natural rights are the rights that impose freedom without any disruptions or interference and the only imposed obligation on the people is in fact the right to not interfere with other people it is also often understood as the right to "life, liberty, and the pursuit of happiness" (Baase, 2012). Many companies however tend to violate the rule and interfere with the happiness of people. As dictated by the law, disruption in any way is in direct violation of the core principle and the fact that the data breach of 2021 (Taylor, 2021) disrupted their customers by instilling a sense of peril as a byproduct of the data leak is a travesty.

- **Inability to contribute to society**

  Societal obligation is personal obligation and when it comes to contributing to the society, virtuous life can be achieved as a by-product of virtuous acts according to Aristotle (Baase, 2012). In a professional environment, it is the job of professionals to aid people with less professional skills. However, LinkedIn came short of performing the primary act of virtue. LinkedIn also failed to protect their clients which should have been the main focus of professionals as their job is to aid people with lesser skillsets than them, as dictated by ethical rule (Baase, 2012)..

- **Disregard for the golden rule**

  A decision is considered to be ethical only when the perspectives of all the parties involved are thoroughly understood (Baase, 2012). In order to make an ethical decision, it is essential that a person or organization take into consideration the various facets of a person's situation (Baase, 2012). The complete disregard for people's livelihoods from the perpetrator's perspective whilst leaking the personal data of millions of people in the case of LinkedIn is utterly despicable if the rules are to be believed in.

- **Opposition to Utilitarianism**

  Utilitarianism emphasizes on happiness and when certain acts are performed, it determines whether an individual is happy or not (Baase, 2012). 'Utility' is what satisfies personal needs and values when it comes to people (Baase, 2012). The situation of LinkedIn serves the function of being a perfect example of violation of utilitarianism as the situation directly contributed to making several of the impacted customer's paranoid, directly affecting their happiness.

Overall, ethics are extremely essential as they aid a profession and the professional and when ethical rules are devalued and debased. It is understood that the entity has no regard for their profession.

6) Professional Issues

An IT professional must follow certain rules that they have to uphold as a part of the IT profession to create a safe and creative environment in their workplace and to anonymously oversee confidential information that the company or a client directly or indirectly provides. An organization that makes sure IT professionals stick to the rules is British Computer Society (BCS) that provides a set of rules and responsibilities that the members embedded within their system must follow (Weiss, 2003). Another one is ACM. The various rules as dictated by the two organizations are:

- **Having regard for public security and wellbeing of others**

  In a professional environment, IT professionals should have regard for public security and wellbeing of others and the environment. In the case of LinkedIn, this was not upheld. LinkedIn was clearly lacking in terms of security that caused an unsanctimonious entity to exploit their customers. This means that the company was unable to follow the rule of conduct (British Computing Society, 2018).

- **Violation of customer trust and dishonesty**

  According to the general ethics principles of ACM, honesty is key and the most essential component of trustworthiness. And when it comes to LinkedIn, the company actively tried to downplay the severity of the situation and in fact had it not been for privacy restore (Taylor, 2021), the situation might just have gone unreported when they expressly advertise their privacy standards (LinkedIn Corporation, 2020). This is in direct violation of the entities embedded within the framework of ACM (ACM, Inc, 2018).

- **Inattention to data security**

  Data security is a major issue of concern or at least should be for multi-national companies such as LinkedIn that exclusively cater to customers and their data and have privacy as one of their main selling points. However, in accordance with the Professional Leadership Principles of ACM that are imposed on every working professional embedded within their system, there should be a certain level of professional concern for customers and their data and there must be rules in place to assure that their data is safe (ACM, Inc, 2018).

- **Honor Confidentiality**

  Confidentiality of information is a fundamental aspect of honesty specially when one has implicitly or explicitly made a promise to honor it (Baase, 2012). Ethical concern is to respect obligations of confidentiality to employers, clients, and users unless the law is involved and while LinkedIn was not solely responsible for the data breach, they contributed to the incident due to exploitable vulnerabilities on their side.

Professionality is the most essential component of a professional and every professional regardless of their profession have sever set of rules that they must oblige to. LinkedIn however came short in several instances and as a by product disrupted several professional rules as explained in the paragraphs above.

7) Personal Reflection

There is a huge discrepancy when it comes to a company's assurance of privacy and their actual real-life implement ability. The company advertises an innocuous version of their actual strategy and plan of action when it comes to catering to privacy needs of their customers. LinkedIn in that way is a direct offender. The company violated their customers' and their right to privacy by not strengthening their security standards when that is what the company expressly advertises.

Competition is the most influential factor of making people. A competitor of LinkedIn, zip recruiter has various policies in place, governing job advertisers and other parties to protect vital data associated with customers against accidental loss, destruction, or damage. Adobe, a company known for its creative products such as Photoshop and Illustrator uses encryption to protect sensitive information and has strict access controls to ensure that only required personnel can access customer data (Greenley-Giudici, 2023). This is based off of Sagefrog's 2022 B2B Trusted Brands Report. The report evaluated various companies according to pre-set criteria that most of the industry is reliant upon and claims to have implemented. It also takes into consideration the views of various customers. Another one of reasons why LinkedIn was not able to protect their customers was due to professional unaccountability and incompetence. This is a major issue in the industry where various leaks and scandals that are scarcely reported on by the company. However, when it comes to the peers of LinkedIn a similar scandal on the same scale has yet to be replicated. This clearly indicates that LinkedIn at that time was lacking in terms of bleeding edge privacy technology as promised when it should have done so. Ethically, the action of the company to downplay the severity of the situation comes across as being extremely unprofessional and rude towards their customers. Some additional information that shows the professional inadequacy on from the side of LinkedIn are lack of transparency, lack of express interest in protecting their customers, lack of respect for professional environment, lack of inadequate security measures, lack of professional accountability. There is no measure of the level of damage that the incident caused the company but the fact that it was unable to protect their seven hundred million customers is not a particularly raving issue.

LinkedIn should have emphasized on improving their security standards and now even though the incident may be outdated, it is still something the company could have not worked on. The ways in which LinkedIn could have improved their security standards and improve privacy are

maintaining transparency, restricting the amount of third-party access, improving their social standing in people's eyes by admitting to wrong doings and not hiding the severity of the situation, not matter how dire the situation is.

References

ACM, Inc, 2018. *ACM Code of Ethics and Professional Conduct.* [Online]
Available at: https://www.acm.org/code-of-ethics
[Accessed 28 April 2023].

Allyn, B., 2019. *22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault.* [Online]
Available at: https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault
[Accessed 8 April 2023].

Baase, S., 2012. ACM Code of Ethics and Professional Conduct. In: M. Horton, ed. *Gift of Fire.* Sand Diego: Pearson, pp. 447-451.

Baase, S., 2012. Ethics. In: M. Horton, ed. *A gift of Fire.* San Diego: Pearson, pp. 26-34.

BORNER, P., 2019. *Data Breach: The Legal Implications.* [Online]
Available at: https://thedataprivacygroup.com/blog/2019-9-17-data-breach-the-legal-implications/
[Accessed 25 March 2023].

British Computing Society, 2018. *BCS Code of Conduct.* [Online]
Available at: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf
[Accessed 28 April 2023].

Bryan Cave, 2016. *2016 DATA BREACH LITIGATION REPORT.* [Online]
Available at: https://www.bclplaw.com/en-US/events-insights-news/2016-data-breach-litigation-report.html
[Accessed 8 April 2023].

Burgess, M., 2020. *What is GDPR? The summary guide to GDPR compliance in the UK.* [Online]
Available at: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
[Accessed 14 April 2023].

corsica technologies, 2020. *PENALTIES AND CONSEQUENCES OF NOT COMPLYING WITH NEW YORK SHIELD ACT.* [Online]
Available at: https://www.corsicatech.com/blog/penalties-and-consequences-of-not-complying-with-new-york-shield-act/
[Accessed 20 April 2023].

Faife, C., 2022. *Seattle hacker gets probation for $250M Capital One data breach.* [Online]
Available at: https://www.theverge.com/2022/10/5/23389266/paige-thompson-seattle-hacker-probation-250m-capital-one-data-breach-amazon
[Accessed 8 April 2023].

Greenley-Giudici, A., 2023. *Data Privacy: What Brands Are Taking It Seriously?.* [Online]
Available at: https://trustarc.com/blog/2023/02/09/data-privacy-most-trusted-brands/
[Accessed 28 April 2023].

Gregersen, E., 2022. *LinkedIn.* [Online]
Available at: https://www.britannica.com/topic/LinkedIn/additional-info#history
[Accessed 26 March 2023].

Hanna, K. T., 2022. *DEFINITION LinkedIn.* [Online]
Available at: https://www.techtarget.com/whatis/definition/LinkedIn
[Accessed 26 March 2023].

LinkedIn Corporation, 2020. *Privacy Policy.* [Online]
Available at: https://www.linkedin.com/legal/privacy-policy
[Accessed 28 April 2023].

LinkedIn Corporation, 2021. *An update on report of scraped data.* [Online]
Available at: https://news.linkedin.com/2021/june/an-update-from-linkedin
[Accessed 30 April 2023].

Nicko,John,Chester , 2023. *LinkedIn Data Leak – What We Can Do About It.* [Online]
Available at: https://scrubbed.net/blog/linkedin-data-leak-what-we-can-do-about-it/
[Accessed 26 March 2023].

oag.ca.gov, 2023. *California Consumer Privacy Act (CCPA).* [Online]
Available at: https://oag.ca.gov/privacy/ccpa
[Accessed 20 April 2023].

Petrosyan, A., 2023. *Annual number of data compromises and individuals impacted in the United States from 2005 to 2022.* [Online]
Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
[Accessed 8 April 2023].

Reynolds, R., 2022. *The Complete History of LinkedIn: Everything You Need to Know*. [Online]
Available at: https://history-computer.com/the-complete-history-of-linkedin/
[Accessed 26 March 2023].

Stouffer, C., 2022. *115 cybersecurity statistics + trends to know in 2023.* [Online]
Available at: https://us.norton.com/blog/emerging-threats/cybersecurity-statistics#
[Accessed 8 April 2023].

Taylor, S., 2021. *New LinkedIn Data Leak Leaves 700 Million Users Exposed.* [Online]
Available at: https://restoreprivacy.com/linkedin-data-leak-700-million-users/
[Accessed 20 March 2023].

Thorsheim, P., 2016. *LinkedIn's poor handling of 2012 data breach comes back to haunt them.* [Online]
Available at: https://www.linkedin.com/pulse/linkedins-poor-handling-2012-data-breach-comes-back-haunt-thorsheim/
[Accessed 20 March 2023].

Weiss, E. A., 2003. *British computer society (BCS).* [Online]
Available at: https://dl.acm.org/doi/10.5555/1074100.1074178
[Accessed 14 April 2023].

Wolford, B., 2023. *What are the GDPR Fines?.* [Online]
Available at: https://gdpr.eu/fines/
[Accessed 25 3 2023].

worldbank.org, 2023. *Data protection and privacy laws.* [Online]
Available at: https://id4d.worldbank.org/guide/data-protection-and-privacy-laws
[Accessed 25 March 2023].

Appendix

STUDENT NAME
Niwesh Dhital Computing

FILE NAME
Niwesh Dhital Computing - plagiarism check 2023

REPORT CREATED
29 Apr 2023

Summary

Flagged passages	2	0.8%
Cited/quoted passages	4	2%

Web matches

trustarc.com	1	0.6%
theverge.com	1	0.5%
statista.com	1	0.5%
ca.gov	1	0.4%
acm.org	1	0.4%
acs.org.au	1	0.4%

Figure3: Originality report for the current report