LINKEDIN
DATA BREACH
STUDY

- Himani Acharya

Table of Contents

Introduction

LinkedIn is a social networking platform owned by Microsoft and founded in 2002, with a motive connecting all the professionals worldwide to make it easy for people to network, find jobs, build and maintain professional relationships, discover career opportunities, and showcase their work history and abilities to others. LinkedIn is like Facebook for professionals but the only difference is it's where people go to network, connect, and find jobs. It is also a valuable platform for businesses to reach the world's largest professional network through job listings that are easy to find. LinkedIn allows businesses to expand their reach and visibility.

LinkedIn was founded by Reid Hoffman and his colleagues Allen Blue, Konstantin Guercke, Eric Ly, and Jean-Luc Valliant who were from well-known companies like PayPal and Socialnet.com.

LinkedIn started its growth as soon as it was launched. As, by 2004 LinkedIn gained 1 million users worldwide. The good news was during this time LinkedIn focused more on improving the user experience not on making more money.

In 2005, LinkedIn then launches Subscription feature which was a success too. LinkedIn premium has a lot more feature and is widely popular till now.

As of now LinkedIn one of the world's leading online social networks for professionals. After Microsoft's investment and purchase of LinkedIn in 2016 it reached to 500 million users worldwide.

Now linked has become the most used for job seekers and business owners. The rise and popularity of LinkedIn not only because it is a social media site but great connections and opportunities through it. (Reynolds, 2023)

Background of the scandal

In recent times, data breaches have become an increasingly common occurrence in the digital world. Unfortunately, even big companies that we trust with our personal information are not immune to these cyber-attacks.

Data breach is considered as unauthorized access of confidential information by someone who do not have access to it. It is a cyber-security Incident. One of the main examples was data breach in Yahoo between 2013 and 2014, later Yahoo forced users to change their password to avoid it later which also caused downfall of Yahoo users and we rarely hear many people using Yahoo in today's context. (Micro, 2023)

One such company is LinkedIn, which experienced a major data breach in June 2021. This incident involved the unauthorized access of personal information of almost every LinkedIn user, which is 700 million people!

The information that was compromised in this breach included names, phone numbers, gender, email address salaries, social media accounts and even details about where people live and work. But financial information and passwords were reported safe. The new dataset of 700 million users was in sale in Dark Web where the hacker had a sample posted of 1 million users for the buyers. This kind of sensitive information falling into the wrong hands can be extremely dangerous and lead to identity theft or other types of fraud.

It's not clear exactly how it happened, but it looks like someone hacked into LinkedIn's computers and took the information. This is a big deal because it means that people's personal information might not be as safe on LinkedIn as they thought.

It was a hacker naked Tom Liner who did the data breach who also stated that he did hacking as a hobby and he had to hack LinkedIn API to get all the user data. He was also the same hacker who did scraping of Facebook's data. (BBC, 2021)

After the incident LinkedIn stated that they will take a legal action against the data scraping and will take the privacy of users very seriously and invest in more ways to protect it.

Legal Issues

Legal issues are the issues of any incident that is concerned with the right and needs to be settled in the court. Legal issues require a legal solution. Parties involved in the case the Plaintiff and the Defendant show proofs and facts to prove or disprove the issue.

Here, LinkedIn is accused of data breach of 700 million users. This can be some of the legal issues concerned with the case:

Violation of data protection laws:

According to the data protection Act 2018 you have right to know what information business and government organisation store about you. (GOV.UK, 2023)

GDPR (General Data Protection Law) was the law drafted by European Union which imposes any organization that collects uses the data collected from any 28 member countries of EU. And any organization who violates the law is fined up to 10 of millions or euros. The GDPR includes consent, breach notification which means the organization should notify the users or owners within 72 hours of the data breach. (Staff, 2022)

The California Consumer Privacy Act (CCPA) is a law that lets people see the information the companies that the companies have saved. This allows the companies to let their customers know what is being done with their data. The consumers can sue the company if they let anybody see their information without permission. Also, you don't have to be a California resident to sue under this new law. (Korolov, 2020)

As the information like name, email, phone numbers, geolocation records, LinkedIn username and profile URL, personal and professional experience, genders, and other social media accounts and details, were exposed, and LinkedIn violated the data privacy and protection law.

Objection with Security Standards:

When it comes to Security standards LinkedIn may have violated security standards including PCI DDS.

(PCI DDS) Payment Card Industry Data Security Standard is a law and security standard by various authorities' and payment card industries like Visa, MasterCard which protects and secures the credit and debit card against various theft. (imperva, 2023)

Though the data breach did not include credit card information. But the potential harm still remains about less security measures to protect other type of security measures in the data breach.

Consumer Protection Law:

Consumer Protection Law is a law enforced to protect all the consumers from fraud or theft in business organization, defective products and goods which they consume. (liberto, 2022)

LinkedIn may also have violated consumer protection law as it failed to fulfill many obligations that they made related to the security and data breach e.g.: It's failure to report the data breach and in time is an also a legal issue to be concerned about.

Also, the unreasonable risk to implement reasonable security measures which result in identity theft and disclosure of personal data of consumers using LinkedIn.

Intellectual Property Laws:

The law which contains the copyright trademark and patent laws for original work like designs, writing, music, photography, films or any type of intellectual creations. When you want to use such creations you need to have a valid copyright law. (Stanford Libraries, 2023)

LinkedIn has the data stored about the users personal and professional experience along with their other social media accounts which has LinkedIn intellectual property rights.

As the information related to personal professional experience was included in the data breach it violates the Intellectual Property Law exposing LinkedIn to legal liability.

Cybersecurity Laws:

Various Cybersecurity Laws like Federal Information Security Modernization Act (FISMA) which has a motive to unsure federal companies use the necessary methods to protect the confidentiality of all the information they go through or store, Cybersecurity Information Sharing Act (CISA) which has a motive to share any cyber threat information and protect data from unauthorized publication was violated by LinkedIn during the data breach. (solutions, 2023)

LinkedIn has the authority to protect the data and prevent it from unauthorized access or publication in any other platform. During the data breach the hacker accessed and published user's data in many other platforms for selling. Also published 1 million user's data just as a sample to show it as a proof which suggests that LinkedIn failed to protect data and take cybersecurity measures.

Social issues

Social issues are the issues recognized by society and has affected the social norms of the society and people which is due to institutional structure of society. Social issues create harm to both social and economic aspects. Those issues are unwanted situations which creates problems and harms to the society.

e.g.: Target's data breach in 2013 included huge number of details of customer including credit and debit cards which then resulted to reputation damage and decline in sales. (connect, 2023)

As LinkedIn is accused of data breach of 700 million users many social issues arose some of them are:

Identity Theft:

Identity theft is a theft of your identity which may include name or any personal information to use it without permission to open new accounts, use it for medical services and many more. Identity theft can lead to financial loss unauthorized charges and many more consequences. Identity Theft might result to betrayal psychological pain of loss and much more to the society. (texasattorneygeneral, 2023)

As during the data breach personal information of millions of people were scraped by the hacker the data and information of the users might have been used by hackers to steal identity or use it for many other services.

Trust issues:

While we involve or invest ourselves in any social media sites for our benefit we do it with a personal trust for e.g.: when a new media or company launches their new product it is difficult to bring it up to public and make them trust with the services. People trust and commit themselves to such products or invention due to their personal trust. But when they can't meet the expectations of trust with their personal and professional information it creates trust issues within the audience.

As LinkedIn is a professional network where the public stores their information with a trust of not being exposed published to unwanted places. The data breach made people rethink about sharing and storing their personal as well as professional information on the network it created a huge trust issue.

Loss of Reputation:

In the year of 2021 advertising revenue of LinkedIn liked and became more than$1 billion also thought to be worth more than $20 billion. The company had many headquarters and many employees across various platforms.

LinkedIn is one of the fastest growing company and was praised a lot because of its unique idea and features but which created a huge reputation across big industries and companies. After the data breach many questions were raised against LinkedIn as being one of the biggest companies and suffering a data breach is very questionable.

The employees of the company had also somehow lost their reputation as their name would be connected with the data breach that LinkedIn suffered from.

Discrimination:

As there was exposure of all the personal information including gender, location in the data breach.

The exposure of all of these data might induce discrimination based on various factors. Targeted attacks to many specific groups through their identity, gender or racial group can lead chances to hate crimes including discrimination and inequality.

Increase of scams and spams:

One of the main social issues which arise from data breach is scam and spams. When personal information such as phone number, email, phone numbers are exposed

This enables cyber criminals to access of so many data to execute scams and spams to which might cause financial loss, physiological as well as emotional effect to individuals.

After the data breach many users of LinkedIn reported many fraud calls and messages. It becomes vulnerable to old people and people with digital illiteracy as they are easy to fall into these type of activities. When these type of data are exposed it becomes easy for cybercriminals to hack into things they want and carry out their operations.

Ethical issues

Ethical issues are those issues concerned with good or bad, right or wrong and that needs a person or organization to choose between them. Sometimes there's a situation where a decision made by a company is chosen on the basis of if it is ethically right or wrong.

e.g.: Google was accused of collecting the data of domestic Wi-Fi networks through street view cars which gave rise to a question about Google's ethical practises.

As LinkedIn is accused of data breach of 700 million users many ethical issues arose some of them are:

Duty of care of data:

Duty of care means a responsibility of the concerned company to have a specific standard of care. This responsibility becomes legal as well as ethical while judging and taking decisions related to the company and the consumers. A failure to keep up the faith and responsibility might also result in legal actions with the law. (kenton, 2022)

LinkedIn being the company to which collects and stores the user data it is the company's ethical duty to avoid the data misuse and to protect it from unauthorised access.

This is a failure of this ethical issue by LinkedIn when data breach included the exposure of all the personal information of users. Being the trusted company with user data it is the responsibility to notify them about the data breach.

As LinkedIn failed to meet the expectations of duty of care this might've brought many legal actions against LinkedIn.

Data Privacy:

Data Privacy simply means the right of an authority to determine when and what type of their personal information do they want to share about themselves. Various type of social media platform collects and store our data and their duty is to keep it safe. But in some cases like data

breach due to companies less security our data gets exposed which leaves us with less privacy. (Cloudflare, 2023)

Here in LinkedIn data breach all the personal information was exposed with violated the data privacy of users which might have brought many bad consequences for the users.

While LinkedIn responded that no personal information was released but it included phone numbers and email addresses is also a violation of privacy.

Regulatory compliance:

Regulatory compliance is all the rules set that an organization needs to follow in order to protect crucial information stored by them. All the organization that work under health, communication, employee safety, data need to follow regulatory compliance. Those who fail to set the rules will be fined. (proofpoint, 2023)

The company should notify the user and prevent from unauthorised access. In this case of LinkedIn, the company has violated by failing to have resources to protect the user data.

Impact on public and professional life of users:

All the professionals that use LinkedIn use it to connect, make networks, find employees, and build their careers. The data breach releases many user's professional information which includes their interest in platforms, jobs, careers and their professional relationships. Which makes the user hesitant to share and upload information to social sites. This has a significant impact on the user's career and reputation.

Now after the breach many users might hesitate to use the platform which impacts on LinkedIn business.

Transparency and disclosure:

At first LinkedIn forcefully denied about the data breach and called it to be fake but instead called it a data scrape and it is not their fault.

Even if the data didn't contain any financial records like: credit, debit card the personal data contained all the details that could lead to scam including phishing attacks, theft, those data leading to advertisement organizations could make it a mess.

This also raises ethical issue regarding the transparency of company. They need to be honest and true whenever any security incidents occur which affect the users are claimed by many authorities.

Professional Issue

It is difficult to provide an understanding of what professionalism means. Being well at work requires being professional. It includes things like dressing appropriately for work or producing outstanding work or obeying the and many other things. Honesty and integrity, responsibility and dependability, self-control and respect, suitable appearance, competence in their function, a solution-focused attitude, and specialized knowledge in their line of work are all characteristics of professionalism. (futurelearn, 2023)

Fiduciary duty:

Fiduciary duty is a duty which is referred in business context where the company has to act on the interests and value of consumers, customers and stakeholders. (sember, 2023)The ethical responsibility to behave solely in the other party's best interests and on their behalf. Fiduciary refers to the party that is in charge, and beneficiary refers to the party that benefits. Professionals always carry out their fiduciary responsibilities.

LinkedIn being a company handling and storing data of million and billion individuals has a relation with them and it is their fiduciary duty to work on the best interest of the users.

But as the data breach was recorded this shows they chose to neglect this duty whether it was knowingly or unknowingly.

Communication:

Communication is very crucial in terms of big businesses, investment or even in a small group of people to make things work out. While a big issue like data breach was conformed in LinkedIn it is important to address and communicate about the issue as it helps to manage the effect to the company as well as the individuals. But the company’s response as something else then what we expected they denied and called it as a violation of terms and service through data scraping. This response of LinkedIn was criticized a lot for failing to admit the data breach as it had a huge impact on the audience.

Crisis Management:

Crisis management is other crucial professional issue which is important while any big crisis or incident occurs in any type of industry. While a big crisis like data breach occurs in a worldwide renowned company like LinkedIn it is their main duty to have a talk, discuss and give a comprehensive response about the crisis and try to manage it as quick as possible. The company should take actions at a very fast pace to investigate about the case and notify all the users to make them safe during the period e.g.: asking them to change their passwords, asking them to keep security authentication. Failure to implement strategies like this can cause bad consequences to company like: financial loss, reputation etc.

Business disorganization:

A data leak disrupts a company's routine operations. LinkedIn's routine business operations, as the company might require more sources and management to work on the breach, such as allocating resources to address the breach, investigating the occurrence, and implementing security measures to avoid future breaches.

This could have an impact on LinkedIn's ability to offer services on timely manner and meet its own objectives or plans which might bring many operational challenges.

Rebuilding trust and reputation:

Trust and reputation is one of the most crucial things of professionalism In business which is vital for their survival and sustainability and brand image. After a big issue like data breach it makes it quite hard for a company to rebuild trust among its users as it might get many losses of the users and its reputation in the future.

To rebuild it a company should be transparent about the breach share its causes and consequences to avoid it in the future not only in their firm but also as a help to other firms. They should take a full accountability about the issue and readdress it to users to make it more secure in the future. Also they should try to rebuild many functions of the site and change needed operations.

Personal reflection

Having heard about data breach incidents, but I never really gave so much attention to it as I hadn't been one of the victims of it. Being someone who limits the use of social media platform and keeps her credentials very secure I am very known about the cybercrimes scams going around in many online platforms regularly.

But thinking about how a data breach could expose my personal information and how that could be used for bad things it is very unsettling for me. Not only would I be impacted, but so would the company that suffered from the incident.

This data breach exposed the details about almost all the users of LinkedIn which is a bit shocking as it included names, phone numbers, gender, email addresses, salaries, social media accounts, and details about where people live and work. All of this information getting into the wrong hands can be disastrous, since I believe data is the most valuable in today's modern world, bringing a lot of beneficial insights when used properly but also being misused in a very horrible way.

Reflecting on the legal issues which the LinkedIn violated including GDPR, data protection laws and more. It is important for a big company like LinkedIn to comply with such laws. The social issues like identity theft, trust issues that arise from the data breach can lead to financial loss. It is also realizable that the data breach could lead to stolen identities of many people. Also, the ethical issues as it is an ethical duty of any firm to protect the users' data. Reflecting on professional issue it also shows how professionalism is very important while such issue crisis arises in any company.

Both people and organizations have a part to play in ensuring individual data, and the results of a breach be dangerous. At last, reflection of an issue is important as it helps us to be more careful within the future and take steps to secure our individual data.

Bibliography

BBC. (2021, 7 16). *BBC*. Retrieved from BBC: https://www.bbc.com/news/business-57841239

Cloudflare. (2023, 4 23). Retrieved from Cloudflare: https://www.cloudflare.com/learning/privacy/what-is-data-privacy/

connect, c. (2023, 4 22). *card connect*. Retrieved from card connect: https://cardconnect.com/launchpointe/payment-trends/target-data-breach#:~:text=In%202013%2C%20the%20infamous%20Target,credit%20and%20debit%20card%20numbers.

futurelearn. (2023, 4 23). Retrieved from futurelearn: https://www.futurelearn.com/info/courses/professional-etiquette/0/steps/225294

GOV.UK. (2023, 4 21). Retrieved from GOV.UK: https://www.gov.uk/data-protection

imperva. (2023, 4 23). *imperva*. Retrieved from imperva: https://www.imperva.com/learn/data-security/pci-dss-certification/

kenton, w. (2022, 4 23). *investopedia*. Retrieved from investopedia: https://www.investopedia.com/terms/d/duty-care.asp#:~:text=minimize%20their%20taxes.-,What%20Is%20Duty%20of%20Care%3F,in%20a%20reasonably%20prudent%20manner.

Korolov, M. (2020, 7 7). *csoonline*. Retrieved from csoonline: https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html

Labs, M. (2021, 6 30). *Malwarebytes Labs*. Retrieved from Malwarebytes Labs: https://www.malwarebytes.com/blog/news/2021/06/second-colossal-linkedin-breach-in-3-months-almost-all-users-affected

liberto, d. (2022, 9 22). *investopedia*. Retrieved from investopedia: https://www.investopedia.com/articles/pf/10/know-your-consumer-protection-laws.asp

Micro, T. (2023, 4 20). *Trend Micro*. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/definition/data-breach

proofpoint. (2023, 4 23). *proofpoint*. Retrieved from proofpoint: https://www.proofpoint.com/us/threat-reference/regulatory-compliance

Reynolds, R. (2023, 4 20). *HistoryComputer*. Retrieved from HistoryComputer: https://history-computer.com/the-complete-history-of-linkedin/

sember, b. (2023, 1 31). *legalzoom*. Retrieved from legalzoom: https://www.legalzoom.com/articles/understanding-fiduciary-duty

solutions, e. e. (2023, 4 22). *enterprise engineering solutions*. Retrieved from enterprise engineering solutions: https://www.eescorporation.com/cybersecurity-laws-and-regulations-in-us/

Staff, O. (2022, 12 14). *Osano*. Retrieved from Osano: https://www.osano.com/articles/data-privacy-laws

Stanford Libraries. (2023, 4 22). Retrieved from Stanford Libraries: https://fairuse.stanford.edu/overview/introduction/intellectual-property-laws/

texasattorneygeneral. (2023, 4 22). *texasattorneygeneral*. Retrieved from texasattorneygeneral: https://www.texasattorneygeneral.gov/consumer-protection/identity-theft/what-identity-theft