Module Code & Module Title

CS5052NI Professional Issues, Ethics and Computer Law

Assessment Weightage & Type

60% Individual Coursework

Year and Semester

2021-2022 Spring

Student Name: Sarthak Bikram Rana

London Met ID: 20049228

College ID: NP01NT4S210129

Assignment Due Date: 12th May 2022

Assignment Submission Date: 12th May 2022

Word Count (Where Required): 3477

I confirm that I understand my coursework needs to be submitted online via Google Classroom 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.

Acknowledgement

This is the first coursework in the Professional Issues, Ethics and Computer Law module, in which we were given to perform the case study on one of the major data breach issue faced by an search engine platform from the recent years. We performed a detailed research on the scenario and explained it on the report along with LSEP issues arrised by it. I had to undertake research on the issue for my coursework by looking at a variety of related articles, journals, reports and websites.

Finally, I’d like to express my gratitude to Ms, Yunisha Bajracharya my respected module leader and Mr. Sandesh Gurung, my respected tutor for introducing me to the topic of Professional Issues, Ethics and Computer Law, introducing me to the sci-hub, where I was able to access various journals and reports to gain a better understanding of the topic, and helping me by reviewing my coursework at various points.

Abstract

The primary purpose of this coursework is to complete a case study by thoroughly researching the issue using numerous reports, journals, publications, and websites. According to the coursework requirements, an introduction portion was provided that generally exposes us to the scenario and what Elastic Search is. The three different scenarios are then elaborated in full with relevant sources in the background of the scandal section.

The fundamental purpose of this module was met in this coursework by the legal, social, ethical, and professional issues commonly referred to as "LSEP." The legal issues were clarified by mentioning the recognized issues in relation to any act or law that was violated as a result of this controversy. The social issues are the effects of these issues on society, people, and even the online casino organization. The ethical issues were discussed by comparing them to all four ethical theories, and the professional issues were explained by offering particular professional code of conduct points that they breached throughout the breach period. At last the conclusion section consists of my personal recommendations and suggestion on how could have the damage of the scandal could have be minimized.

Table of Contents

List of Figures

1. Introduction

The first case occurred in January 2019, where a huge data leak issue of an online casino business occurred as a result of the Elastic Search server being exposed online without any kind of passwords. Due to the data leak, ZDnet, a cyber security news outlet, issued an article on the incident in which it stated that the server was exposed for an long period of time, affecting many of its users.

The second case explains that this is not the first time an Elastic Search database breach has occurred, but this breach was the largest of all, resulting in the exposure of approximately 5,088,635,374 records after a UK-based security company accidentally exposed its database containing information related to security incidents between 2012 to 2019.

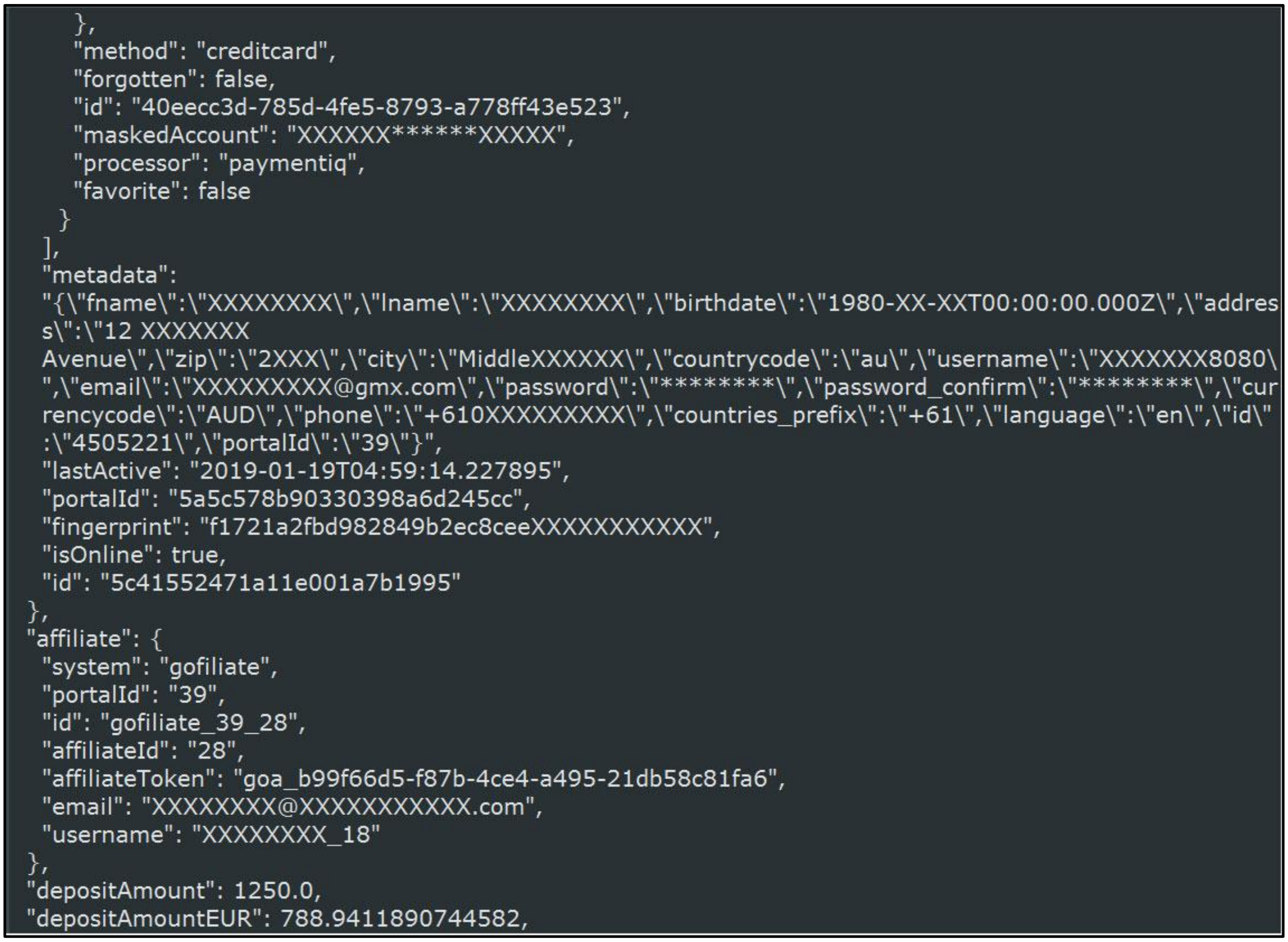
The third and final case elaborates on the previous ElasticsSearch incident, which occurred in March 2019 when an app developer from an organization left its database open, which contained more than 70 million log files containing 100 gigabytes of data stored, from which the exposed data included details about the device data, links to photos and videos, and around 800,000 email addresses.

The Elastic search is an open source analytics and full-text search engine, which is used for enabling search functionality for applications. Through Elastic search, we can build complex search functionality, similar to what we see on Google. This includes auto-completion, correcting typos, highlighting matches, handling synonyms and adjusting relevance. We can also query structured data such as numbers and aggregate data, and use Elastic search as an analytics platform. It can do everything which will need to build a powerful search engine (Divya & Goyal, 2013).

The working mechanism of Elastic search is the data are stored as documents, which is just a unit of information. A document in it corresponds to a row in a relational database, and can represent a person, a sale, or anything else you want. A document then contains fields, which correspond to columns in a relational database. It is being used by large companies, also there are many other users of it and there is a vibrant community. It is by far one of the biggest name in terms of search engines (Divya & Goyal, 2013).

2. Background of the Scandal

The first scenario occurred in 2019 January, where Justin Paine who is the security researcher found out an unsecured ElasticSearch database was discovered exposing the details for over 108 million bets at various online casinos such as azur-casino.com, easybet.com, skates.com, viproomcasino.com, casinogym.com, crazyfortune.com, luckyluke.com and kahunacasino.com. The leaked information contained numerous details including the customer's personal information which includes bettor's name, address, partial credit card numbers, email addresses, the bet amount including deposits and withdrawals (Lawrence Abrams, 2019).



```
      },
      "method": "creditcard",
      "forgotten": false,
      "id": "40eecc3d-785d-4fe5-8793-a778ff43e523",
      "maskedAccount": "XXXXXX******XXXXX",
      "processor": "paymentiq",
      "favorite": false
    }
  ],
  "metadata":
  "{\"fname\":\"XXXXXXXX\",\"lname\":\"XXXXXXXX\",\"birthdate\":\"1980-XX-XXT00:00:00.000Z\",\"addres
  s\":\"12 XXXXXXX
  Avenue\",\"zip\":\"2XXX\",\"city\":\"MiddleXXXXXX\",\"countrycode\":\"au\",\"username\":\"XXXXXXX8080\
  ",\"email\":\"XXXXXXXXX@gmx.com\",\"password\":\"*********\",\"password_confirm\":\"*********\",\"cur
  rencycode\":\"AUD\",\"phone\":\"+610XXXXXXXXX\",\"countries_prefix\":\"+61\",\"language\":\"en\",\"id\"
  :\"4505221\",\"portalId\":\"39\"}",
  "lastActive": "2019-01-19T04:59:14.227895",
  "portalId": "5a5c578b90330398a6d245cc",
  "fingerprint": "f1721a2fbd982849b2ec8ceeXXXXXXXXXXX",
  "isOnline": true,
  "id": "5c41552471a11e001a7b1995"
},
"affiliate": {
  "system": "gofiliate",
  "portalId": "39",
  "id": "gofiliate_39_28",
  "affiliateId": "28",
  "affiliateToken": "goa_b99f66d5-f87b-4ce4-a495-21db58c81fa6",
  "email": "XXXXXXXX@XXXXXXXXXXX.com",
  "username": "XXXXXXXX_18"
},
"depositAmount": 1250.0,
"depositAmountEUR": 788.9411890744582,
```

Figure 1: Example of how data are stored in the database (Lawrence Abrams, 2019).

All of the consumers sensitive information was saved in a single server by ElasticSearch, which managed a massive collection of data gathered from many web domains, most likely through some sort of affiliate scheme or a larger corporation managing multiple betting portals. Paine and ZDNet concluded that all domains were running online casinos where users could place bets on classic card and slot games, as well as other non-standard betting games, based on a review of the URLs discovered in the server's data. Some of the domains were registered by the same company, but others were owned by companies based in the same building in Limassol, Cyprus, or were operating under the same eGaming license number granted by the government of Curacao, a small Caribbean island (Catalian Cimpanu, 2019).

According to Paine, 108 million records containing information on current bets, wins, deposits, and withdrawals were present on that server at the time of the data breach. He also stated that the payment card details in the ElasticSearch server were partially extracted, not exposing the user's full financial details and that if anyone found the database open at the time, that individual would have known all the personal information about the online casino group's customers, which anyone could have used to target users as part of various scams or extortion schemes (Catalian Cimpanu, 2019).

In the second scenario, a security researcher named Bob Diachenko discovered the most significant data breach to date on the same ElasticSearch server. The data was identified as belonging to Keepnet Labs, a UK-based security company that focuses on safeguarding organizations from email-based cyber-attacks. It provides data gathered from security incidents that occurred between 2012 and 2019. Bob claimed that there were two different sets of data within the database, one with 5,088,635,374 entries and another with 15 million records, from which the five billion were exposed. Bob stated that the data was well-structured, with the hashtype, leak year, password (hashed, encrypted, or plaintext, depending on the disclosure), email, email domain, and source of the breach all included. After he discovered the problem and immediately notified Keepent Lab, the database was taken offline within an hour to prevent any data loss (Arghire, 2022).

Talking about the third scenario of the ElasticSearch server leak incident which was occurred due to the negligence of an individual named Bithouse who was an app developer of the mobile app known as Peekaboo where he left the ElasticSearch database open which consisted of 70 million log files comprising nearly more than 100GB of data stored from March 2019. Those data consisted of 800,000 email address, detailed device data often, links to photos and videos, all of which get stored on servers stored by Singapore based Alibaba Cloud. Later, Peekaboo stated that they were still unclear for how long the server was exposed to the pubic and if anyone had accessed it or not (Kirk, 2020).

3. Legal Issues

A legal issue is something that occurs and has legal consequences and may require the assistance of a lawyer to resolve it (Solicitors Regulation Authority, 2021). The ElasticSearch has faced several legal issues due to its leaky server. Some of them are as follows,

Data Breach Notification law:

According to the various states in the United States of America that have passed the "Data Breach notification law," which requires state residents to be notified of a security breach involving more sensitive categories of information, such as Social Security numbers and other government identifiers, credit card and financial account numbers, health or medical information, insurance ID, tax ID, birthdate, as well as online account credentials, digital signatures and biometrics (dlapiperdataprotection, 2022).

In this sceneriao, according to this law it is an compulsion that any kind of organization or company shoud notify its customers if it faces any kind of cyber security issues. Where one of the biggest search engine globally known as ElasticSearch were not able to identify that they have an exposed server which is an big legal issue and they were not able to inform their customers about it.

Data Privacy Act:

Due to the possible missues of personal data over the internet, the Data Privacy Act consists of various significant rights and restrictions on data stored by US government entities. Because the company ElasticSearch has experienced data leaking from its server several times, as described in the scenario which demonstrates that they have not been following to the data privacy act instead violating it, which is a serious concern. The company should reform its privacy law timely manner in order to improve its network security to prevent such incident from occurring again.

Electronic Communications Privacy Act:

The Electronic Communications Privacy Act (ECPA) is a federal law in the United States that prevents third parties from eavesdropping or exposing communications without authorisation. The Act, which began as an amendment to the Wiretap Act of 1968, applies to both government employees and private persons. It safeguards communications both in storage and in transit (TechTarget, 2022).

According to the various scenarios described above, it can clearly observe that the ElasticSearch search engine's server had data breaches on multiple occasions, most of which they were unaware of. The company definitely breached the Electronic Communications Privacy Act as a result of the data leak. The server held sensitive customer information such as emails, name, address, credit card information, transactions, leak date, source of the leak, hashtype, links to photographs and videos, and many more. The act also specifically prohibits any third party from intercepting or disclosing communications without authorization, however due to the data leak anyone may have gained access to those various datas, resulting in a massive cyber crime.

Computer Security Act:

The Computer Security Act is an early attempt to establish security standards for the next generation of computers. This act also mentions that all computer systems that contain classified information must have security plans in place, and that all people who operate, design, or manage those computer systems must receive periodic security training.

From the all data breach incidents which the company ElasticSearch faced they were all due to its leaky server and the app developer of the Peekaboo had bad practice of the security training. Comparing to the act it can be clearly observed that the company didn’t applied any kind of security plans which includes implementation of firewalls in its server and the app developer had the bad practice of leaving the database open. Thse activiry clearly states that the company and the individual has also violated this act.

Children Online Privacy Protection Act:

The purpose of the Children Online Privacy Protection Act (COPPA) is to safeguard all children under the age of 13 from the negative aspects of the internet. According to the third scenario provided in this coursework, the ElasticSearch database was left open by the Peekaboo company's app developer, which consisted of access to photos and videos of all children under the age of 13.

Because of the bata breach in ElasticSearch's leaky server, the photos and videos of children were all left open on the internet, where anyone could have gotten access to them and misused them in the wrong way, which is against the Children Online Privacy Protection Act, which clearly states that the company has also violated this act.

4. Social Issues

A social issue in terms of cyber security any kind of social difficulties that arrises due to any kind of carelessness of the organization or different cyberattacks. The ElasticSearch might have faced several social issues due to the data breach. Some of them are as follows,

Affect on Users:

The data breaches which occurred to the ElasticSearch database has compromised three different companies, one to the online casino business where more than 108 million datas were leaked, another one where the U.K. based security company exposed its database which consisted 5 billion sensitive informations and the last one where an app developer of an app named Peekaboo left the database open which consisted 70 million files.

Due to the data breach, the valuable informations such as their names, home address, phone numbers, email, credit card information of users, sensitive informations related to security incidents and photos and videos of childrens were exposed to the internet where any one could have misused it, which could have affect the users in the wrong way both mentally and physically.

Vandalism:

The ElasticSearch data breach leaked personal information of a lot of its customers including from the users of online casino group, U.K. based security company and Peekaboo application. Those information consisted the user names, home address, phone numbers, email, credit card information of users, sensitive informations related to security incidents and photos and videos of childrens. Criminals can simply conduct many crimes using a false social security number if they have access to such vital information. Innocent people's information can be exploited for various illegal actions because their credit card information was also included in the database, which kept the true criminal hidden from the world.

Identity theft:

The ElasticSearch data breach exposed the personal information of many of its customers to several types of potential dangers. These details included user names, home addresses, phone numbers, email addresses, credit card information, sensitive information about security problems, and images and videos of youngsters. Such information can easily be utilized for unlawful actions. For example, with such information, anyone can commit identity theft by impersonating another person. Following the breach, there could be numerous cases of identity theft.

Faliure of providing service:

When ElasticSearch experienced a data breach, it affected many customers because the hack compromised their valuable and sensitive data, exposing it to the internet. The organization experienced both traditional service failures caused by the app developer and online service failures caused by its leaky server, which was breached many times, violating data security and privacy. Because of these concerns, it is clear that the company failed to meet the terms and conditions and violated the trust of their precious consumers. These could have long-term consequences on consumer views of service quality. Customers perceptions of service quality may suffer if they perceive their information is unsafe with a company.

Future Expectations:

The data leak has had a significant impact on both the corporation and its customers. Since Elastic Search has experienced repeated data breaches and has been unable to detect and mitigate vulnerabilities in their system, the company's value and image in the market have suffered. Customers may think that the company may face similar challenges in the future, causing them to lose faith and as a result, they may stop using Elastic Search services in the future.

5. Ethical Issues

An ethical issue in terms of cyber security any kind of situation where the moral standard is questioned (Vallor & Rewak, 2018). The ElasticSearch and the victims of the breach might have faced several ethical issues due to the data breach. Some of them are as follows,

Virtue Theory

The virtue theory focuses on one's qualities or moral character rather than one's obligations, laws, or consequences. Since Elastic Search's server housed valuable and sensitive data from its various customers, and they were not implementing any kind of firewalls in their server over time without considering the consequences that they would face. Customers placed their trust in them, and they have the right to expect that the information they provide will be kept private among those to whom it was initially revealed in these types of transactions. Because the information was leaked to third parties, the corporation failed badly in its moral obligation and can thus be accused of not adhering to the idea.

Deontology

The deontological theory uses set of rules to distinguish right from wrong. Since the Elastic Search failed to protect its servers form data breaches it clearly breaked the trust of its customers, their image in the market and the industry regulations against keeping all sensitive and valuable datas from access to any individual from public. Since they faced similar issues in the past, they were never able to distingusish what is right from wrong by applying mitigation strategies such as strong firewalls for their leaky servers.

Utilitarinism

Since the organization has experienced repeated data breaches as a result of their leaky server, which stored their users important and sensitive data. The corporation broke the utilitarian concept of "most value to the most people" by exposing such a large amount of information about millions of people. The company's lack of data security will deter present and future consumers from utilizing that platform because they are not receiving any type of advantage and it is impacting their happiness, nor are they receiving any kind of compensation.

Rights

One of the ethical theories that Elastic Search has breached is the concept of rights. The company violated its consumers right to privacy by compromising their valuable and sensitive data. The many platforms maintained trust in the Elastic Search servers by storing sensitive data, yet the company was unable to secure and respect their consumers' privacy rights. Elastic search has violated not only their own agreements by releasing such massive amounts of data in such a casual manner, but they have also violated people' fundamental right to privacy and the ethical principle on which they are established.

Transparency:

Elastic Search has responsibilities to its users because it is a large internet search engine with a large number of active users. As described in the scenario, they have had repeated data breaches and are completely unaware of it. It is also stated that cyber security experts from third-party businesses learned about the incidents and notified them. It is the company's responsibility to establish security measures in order to mitigate such difficulties, as well as to notify its customers if such a situation arises. They did not inform their clients about their situation in this case. Such conduct is unethical and in violation of numerous consumer laws. They chose to hide the truth from their consumers rather than pursue a business policy that also violated transparency.

6. Professional Issues

A professional issue in terms of cyber security any responsibility of decision-making, confidentiality, privacy, piracy, fraud & misuse, liability, copyright, trade secrets, and sabotage are all security issues that a company may face (Vallor & Rewak, 2018). The Elastic Search and the victims of the breach might have faced several professional issues due to the data breach. Some of them are as follows,

Codes of Conduct and Behaviour:

Due to many large data breaches that exposed personal information about its consumers, it generally violated the standards of conduct and behavior. To avoid this, the company's employees must continually ensure that public data security and privacy are not jeopardized in any situation involving public data security or privacy. Codes of conduct can act as both a guide and a safeguard. The firm, on the other hand, failed to provide both safety and training, as well as compensation, resulting in a violation of behavioral standards.

Hiring unqualified officials:

Elastic Search is a significant search engine in the United States that has previously had multiple data breaches. Because of the breach, sensitive and valuable information about their consumers was exposed on the internet. This breach exposed almost 5 billion records in total. Anyone with access to the data could have misused it as a result of the breach. This circumstance arose as a result of the company's leaky server and individuals' poor cyber security practices. The organization lacked highly qualified authorities who could implement firewalls in its servers and knew what to do after an attack, such as an emergency response strategy, mitigation measures, breach notification, and so on.

Community Standards:

The majority of professional groups have codes of conduct or ethics that they follow on a regular basis. Their mission is to support members and to create professional standards. Elastic search has also produced a set of community norms that represent their professional conduct. The firm, on the other hand, appears to have violated its own policies by exposing the server without permission and bypassing all firewalls and passwords. Taking so long to learn about the intrusion displays a lack of integrity and competence.

Delayed report of Breach:

People learned of their loss of personal information from their trusted organization when the case of Elastic Search's data breach was made public. After many third party cyber security specialists became aware of the problem and reported it, it was discovered that the corporation was uninformed of the situation because no preventive measures had been implemented and no one had been hired to prevent such a situation. According to the contract and principles in cyber security, they must notify users of the issue, which is a professional act and their duties.

Violation of Contract:

In terms of legality, companies establish contracts with their clients stating that they will perform services smoothly, safeguard data privacy, and many other things. These contracts are signed and agreed upon to provide certain services while adhering to the business code of conduct. These contracts indicate the company's commitment to acquiring their users' trust. Clients place their trust in them and expect companies to perform successfully in order to keep such promises. In this case, the company was unable to keep its contract due to multiple data breaches.

7. Conclusion

In conclusion, Due to weak cyber security policies, the company's Elastic Search servers containing significant and sensitive data were repeatedly accessed in this case. This is a major concern because they disregarded their clients' confidence and broke their own company standards. Certain security measures may have been implemented by the organization to lessen them.

As a result of these circumstances, the company was confronted with all LSEP difficulties, including various legal issues such as data breach notification law, data privacy act, computer security act, and others, as well as social issues such as vandalism and identity theft. It also has an impact on all ethical and professional issues, such as codes of conduct, integrity, and data misuse.

If Elastic Search had taken various measures, such as always checking and securing the server's default configuration before deploying it and not making it accessible to the public on the internet, the database should always be authenticated by using hashed passwords, and the data inside the server should not be stored in plaintext but rather encrypted using advanced cryptographic measures.

The company should conduct an IS audit in a timely manner to help them uncover various issues, and all of the organization's employees should retain legacy practices; otherwise, stern penalties should be taken against them. These are a few ideas and suggestions from my end for the protection of their server and the precious data of their clients, which can prevent or lessen the occurrence of both data breaches and LSEP issues.

References

Lawrence Abrams, 2019. *Online Casino Database Leaks Details of Over 100 Million Bets.* [Online]
Available at: https://www.bleepingcomputer.com/news/security/online-casino-database-leaks-details-of-over-100-million-bets/
[Accessed 3 May 2022].

Catalian Cimpanu, 2019. *Online casino group leaks information on 108 million bets, including user details | ZDNet.* [Online]
Available at: https://www.zdnet.com/article/online-casino-group-leaks-information-on-108-million-bets-including-user-details/
[Accessed 5 May 2022].

Arghire, I., 2022. *Unprotected Database Exposed 5 Billion Previously Leaked Records | SecurityWeek.Com.* [Online]
Available at: https://www.securityweek.com/unprotected-database-exposed-5-billion-previously-leaked-records
[Accessed 6 May 2022].

Kirk, J., 2020. *Baby's First Data Breach: App Exposes Baby Photos, Videos.* [Online]
Available at: https://www.bankinfosecurity.com/babys-first-breach-app-exposes-baby-photos-videos-a-13603
[Accessed 6 May 2022].

Solicitors Regulation Authority, 2021. *SRA | What is a legal issue | Solicitors Regulation Authority.* [Online]
Available at: https://www.sra.org.uk/consumers/choosing/legal-issue/
[Accessed 7 May 2022].

dlapiperdataprotection, 2022. *Breach Notification in United States - DLA Piper Global Data Protection Laws of the World.* [Online]
Available at: https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=US
[Accessed 7 May 2022].

TechTarget, 2022. *What is Electronic Communications Privacy Act (ECPA)? - Definition from WhatIs.com.* [Online]
Available at: https://searchcompliance.techtarget.com/definition/Electronic-Communications-Privacy-Act-ECPA
[Accessed 7 May 2022].

Goode, S., Hoehle, H., Venkatesh, V. & Brown, S., 2017. USER compensation as a data breach recovery action: An investigation of the sony playstation network breach. *MIS Quarterly: Management Information Systems,* 41(3), pp. 703-727.

Appelbaum, P. S., Kapen, G., Walters, B. & Lidz, C. W., 1984. Confidentiality: An empirical test of the utilitarian perspective. *The Bulletin of the American Academy of Psychiatry and the Law,* 12(2), pp. 109-16.

Petronio, S. & Altman, I., 2002. *Boundaries of Privacy: Dialectics of Disclosure.* Albany, New York: State University of New York Press.

Culnan, M. J. & Williams, C. C., 2009. How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data. *MIS Quarterly,* 33(4), pp. 673-687.

Duquenoy, P., Jones, S. & Blundell, B. G., 2007. *Ethical, Legal and Professional Issues in Computing.* 1st ed. s.l.:Cengage Learning.

Elasticsearch B.V., 2022. *Community code of conduct.* [Online]
Available at: https://www.elastic.co/community/codeofconduct
[Accessed 21 April 2022].

Vallor, S. & Rewak, W. J., 2018. *An Introduction to Cybersecurity Ethics,* Santa Clara: Santa Clara University.

Divya, M. S. & Goyal, S. K., 2013. ElasticSearch An advanced and quick search technique to handle voluminous data. *An International Journal of Advanced and quick search technique to handle vlominous data,* 2(6), pp. 171-175.

Bibliography

Smethers, S., 2016. Cyberspace in the Curricula: New Legal and Ethical Issues. *Journalism & Mass Communication Educator,* 52(4), pp. 15-13.

financierworldwide, 2015. *Cyber security: the dos, the don'ts and the legal issues you need to understand — Financier Worldwide.* [Online]
Available at: https://www.financierworldwide.com/cyber-security-the-dos-the-donts-and-the-legal-issues-you-need-to-understand#.YnzQzC8Rp-V
[Accessed 5 May 2022].

tripwire, 2021. *A Look at the Legal Consequence of a Cyber Attack.* [Online]
Available at: https://www.tripwire.com/state-of-security/featured/legal-consequence-cyber-attack/
[Accessed 6 May 2022].

Appazov, A., 2014. *Legal Aspects of Cybersecurity,* Copenhagen: University of Copenhagen.
Adonis, A. A., 2020. *International Law on Cyber Security in the Age of Digital Sovereignty,* s.l.: s.n.

Liu, E. C. et al., 2020. *Cybersecurity: Selected Legal Issues,* s.l.: Congressional Research Service.

Cisomag, 2020. *Leaky Elasticsearch Database Exposes Peekaboo Moments' Data.* [Online]
Available at: https://cisomag.eccouncil.org/elasticsearch-database-leaks-100-gb-data-of-peekaboo-moments-app/
[Accessed 5 May 2022].

Vskills, 2015. *LEGAL ISSUES IN CYBERSPACE - Vskills Blog.* [Online]
Available at: https://www.vskills.in/certification/blog/legal-issues-in-cyberspace/
[Accessed 7 May 2022].

CCLA, 2018. *"Cyberspace Law" And Web Privacy Violations - CCLA.* [Online]
Available at: https://ccla.org/get-informed/talk-rights/cyberspace-law-and-web-privacy-violations/
[Accessed 7 May 2022].

offthepagecreations, 2022. *Legal Issues on the Internet - Copyright, Cyber Crimes, Spam.* [Online]
Available at: https://www.offthepagecreations.com/legal-issues/
[Accessed 8 May 2022].

Baden, M. S. & Wilkie, K., 2006. *Problem-Based Learning Online.* 2 ed. New York: Open University Press.

Kizza, J. M., 2003. Ethical and Social Issues in the Information Age. In: *Texts in Computer Science.* New York: Springer, pp. 283-321.

Gunarto, H., 2020. *Ethical Issues in Cyberspace and IT Society,* Oita: Ritsumeikan Asia Pacific University .

rainbowtables, 2019. *Online Casino Database Leaks Details of Over 100 Million Bets.* [Online]
Available at: https://rainbowtabl.es/2019/01/21/online-casino-group-leaks-information-on-108-million-bets-including-user-details/
[Accessed 11 May 2022].

Baase, S., 1996. *A Gift of Fire.* 4 ed. San Diego: San Diego State University.