



CC5052NI Professional Issues, Ethics and Computer Law

Contents

60% Individual Coursework

Spring 2024

Student Name: Dikshya Sharma

London Met ID: 22067520

Assignment Submission Date: 5th May 2024

Word Count: 3482

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.

Table of Contents

1. Introduction	1
1. Background	3
2. Legal Issues	5
a. Privacy Laws Violation	5
i. Personal Information Protection and Electronic Documents Act 2000(PIPEDA)	5
ii. Privacy Act (1998)	6
iii. Computer Fraud and Abuse Act(CFFA)	6
b. Court Cases	7
c. Legal Consequences , Fines and Penalties.....	7
3. Social Issues	8
a. Impact on society	8
b. Loss of Reputation and Jobs	8
c. Impact on Relationships and family	9
d. Psychological Consequences and Crimes.....	9
e. Gender Discrimination.....	11
f. Impact on Religious Faith	11
g. Financial loss.....	11
4. Ethical Issues	12
a. Dishonesty and Integrity Deficiency	12
b. Violations of moral justification	13
c. Morality of facilitating infidelity.....	13
d. Right Ethics.....	14
5. Professional Issues.....	15
a. Professional Misconduct	15

b.	Breach of professional contracts	15
c.	Violation of various professional code of conducts	15
i.	Violation of BCS(British Computer Society) Code of Conduct.....	16
ii.	Violation of ACM(Association of Computing Machinery) Code of Conduct.....	16
iii.	Violation of IEEE(Institute of Electrical and Electronics Engineers) Code of Conduct	17
6.	Conclusion.....	18
7.	References	20

Table of Figures

Figure 1: Ashley Madison Landing Page (MILLER, 2023).....	2
Figure 2: Message from Impact Team (KrebsOnSecurity, 2015)	4
Figure 3: Full Delete Feature (Megan, 2015).....	6
Figure 4: Blackmails and Threats after the Breach (Gill, 2020)	10
Figure 5: Blackmails and Threats after the Breach 1.0 (Gendre, 2021).....	10

1. Introduction

The spread of the Internet has completely changed the way people build and maintain personal relationships. With the internet, people can now easily interact with others from all over the world, breaking down geographical barriers that once limited the possibilities of meeting new people through computer-mediated communications. This has greatly impacted the way individuals seek intimate connections through online dating. Dating apps are software programs created to connect individuals interested in friendship, casual dates or romance which offers the chance to meet someone with minimal efforts ([Orchard, 2019](#)). One of the examples of such dating sites is **Ashley Maddison**.

Ashley Madison is a dating website targeted towards people who are married or in relationships but are interested in having discreet extramarital affairs. It was the first popular website for extra marital affairs, originally designed for people in committed relationships who want to cheat on their partners which perfectly fits different lifestyles , widening its network of people. It gained notoriety for its slogan "**Life is short. Have an affair**" and for being a platform that facilitates infidelity. The app was named by combining the names of the most popular girls of 2001 and was first developed and founded in 2001 by Darren J Morgenstern along with Noel Binderman who later became CEO ([AGARWAL, 2023](#)). Its parent company was Avid Life Media which later changed its name to Ruby. The website soon became recognized as the market leader in innovation in the world of technology, driven by its vision to transform online relationships ([O'Brien, 2016](#)).

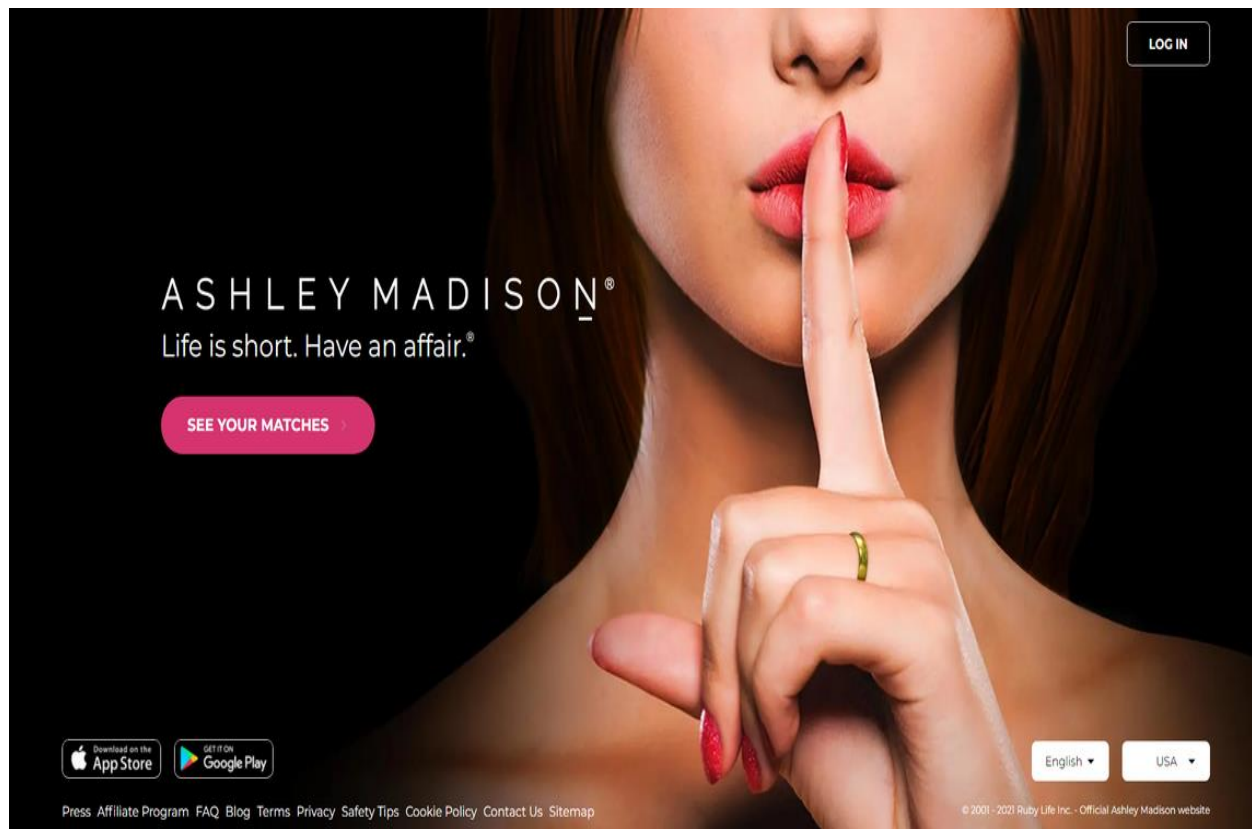



Figure 1: Ashley Madison Landing Page (MILLER, 2023).

1. Background

A data breach is when unauthorized individuals gain access to confidential information, leading to loss, alteration, or unauthorized disclosure of personal data. It occurs when cyber attackers find weakness in the system and launch attacks which not just affect the breached organization but also everyone whose personal information gets stolen (Trendmicro, 2018). One of the most infamous examples of a data breach is the **Ashley Madison incident**.

The Ashley Madison data breach unfolded in series of key events starting from **July 12, 2015**, which was performed by a hacker group calling itself the **Impact Team** that involved loss and theft of details belonging to up to 38 million members. It began with a threatening message from a hacker demanding the shutdown of Ashley Madison and Established Men setting a **30-day deadline**. The hackers proceeded with their threat releasing the first major data dump on **August 18, 2015** containing nearly 10GB of user email addresses. The breach continued and on **August 20, 2015**, a second major data dump was released containing internal data, CEO emails and source code. The data dumps continued with a third round of data leak on **August 23, 2015**, which included a full list of government emails used and user details from specific states. The data dump continued with state-by state leaks of users on **August 25-26, 2015**, which marked the unfolding of one of the largest and most infamous data breaches in history (Lord, 2017).

Unlike other data breaches, Ashley Madison exposed extremely private information unique to a dating website, such as **user's fantasies, sexual preferences, and intimate images**, instead of just **credit card numbers** and demographic information and when asked the motivation behind the breach in an interview with Motherboard via email, they expressed their outrage about the activities allowed on Ashley Madison site, which they saw as promoting **prostitution and human trafficking**. They also criticized Ashley Madison's weak security and failure to **delete user data properly**. They further said, their planning for the attack was started years ago and hence they executed their attack effortlessly due to company's weak security. With no oversight, they can easily access servers using simple passwords like "Pass1234" (Cox, 2015).



AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY

We are the Impact Team.
We have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, emails

Shutting down AM and EM will cost you, but non-compliance will cost you more:
We will release all customer records, profiles with all the customers' secret sexual fantasies, nude pictures, and conversations and matching credit card transactions, real names and addresses, and employee documents and emails.
Avid Life Media will be liable for fraud and extreme harm to millions of users.

Avid Life Media runs Ashley Madison, the internet's #1 cheating site, for people who are married or in a relationship to have an affair. ALM also runs Established Men, a prostitution/human trafficking website for rich men to pay for sex, as well as cougar life, a dating website for cougars, man crunch, a site for gay dating, swappernet for swingers, and the big and the beautiful, for overweight dating.

Trevor, ALM's CTO once said "Protection of personal information" was his biggest "critical success factors" and "I would hate to see our systems hacked and/or the leak of personal information"

Well Trevor, welcome to your worst fucking nightmare.

We are the Impact Team. We have hacked them completely, taking over their entire office and production domains and thousands of systems, and over the past few years have taken all

Figure 2: Message from Impact Team (KrebsOnSecurity, 2015)

2. Legal Issues

This section covers the primary legal issues surrounding the breach, such as liability, data protection and privacy laws and security laws. The subjects that are covered by legal issues are listed below:

a. Privacy Laws Violation

Ashley Madison advertised itself as a secure and trustworthy means for consenting adults to have affair but turns out it was using inadequate privacy and security technologies. People paid money for a relationship as well as for security and privacy, but it was breached which exposed extremely private information.

i. **Personal Information Protection and Electronic Documents Act 2000(PIPEDA)**

Ashley Madison was lacking privacy and security measures despite handling user's sensitive information. The company had **weak authentication** processes, **insecure encryption** and poor key and **password** management. Even though they mentioned “**Full Delete**” feature, personal information were retained even after user profiles were deleted which violates *Personal Information Protection and Electronic Documents Act 2000(PIPEDA)*, Canada's federal private sector private law which governs the collection, use and disclosure of personal information by private sector organization ([Office of the Privacy Commissioner of Canada, 2016](#)).

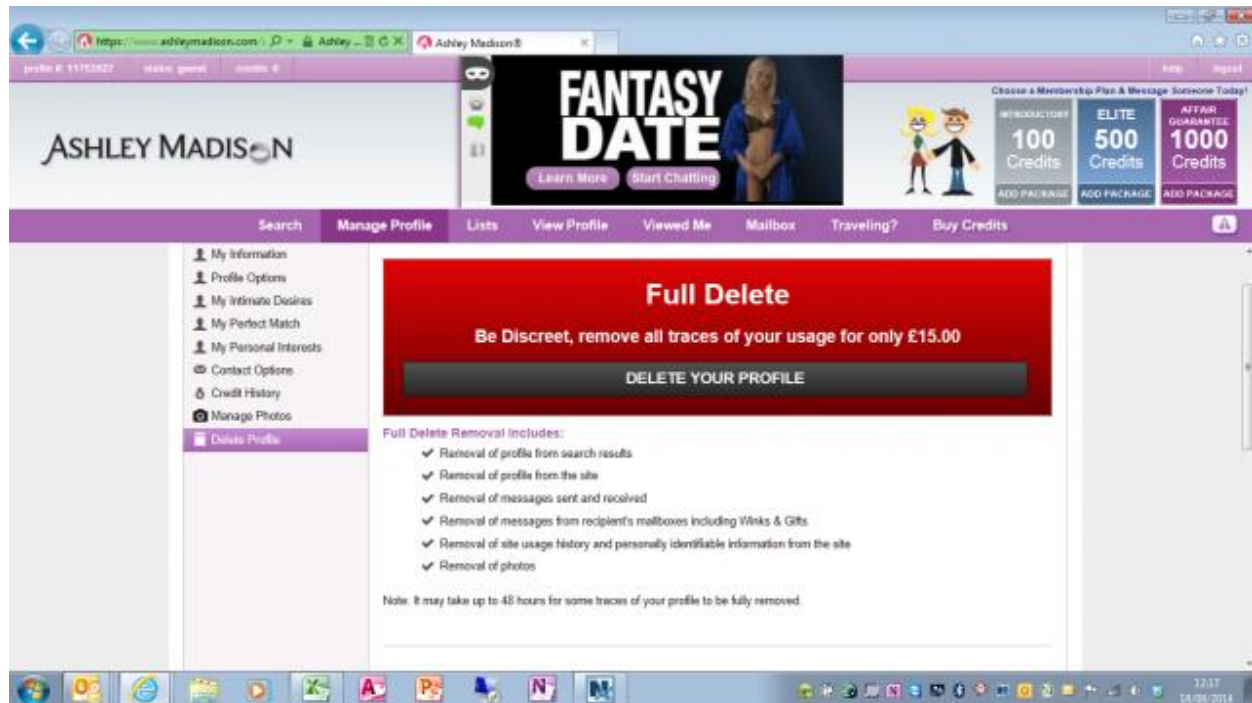


Figure 3: Full Delete Feature (Megan, 2015)

ii. Privacy Act (1998)

Although Ashley Madison was headquartered in Canada, their business was carried in Australia as well and hence they were also collecting information from Australian residents. The company was found collecting personal information like credit card details and more such information's from users and failed to provide transparency to the users about the information collection process which was not considered acceptable under the Privacy Act of Australia. Therefore, Ashley Madison violated Australian **Privacy Act(1998)** (Clifford Chance, 2016).

iii. Computer Fraud and Abuse Act(CFFA)

Impact Team who hacked Ashley Madison leaked 33 million user records which violates **Computer Fraud and Abuse Act(CFFA)**. The CFFA prohibits unauthorized access to computer systems and data, and the action of the hackers that is; Impact Team in this case is considered unauthorized and thus illegal under the CFFA (Wolfe, 2015).

b. Court Cases

The lawsuits against Avid Life, the parent company of Ashley Madison, were indeed numerous and wide ranging. The **class action lawsuits** were boosted in Federal District Courts across the nation. By the end of 2015, roughly a dozen such suits were filed in the US which included breach of contract, negligence, and violation of various privacy laws. Likewise, people **Two Canadian law firms filed a \$578 million class action suit**, alleging inadequate protection of user data regarding “Full Delete” Feature ([Jones, 2017](#)).

c. Legal Consequences , Fines and Penalties

In response to the breach, Ashley Madison agreed to a settlement totaling **\$11.2 million in the US to resolve the class actions lawsuits** filed on behalf of affected individuals ([CBC News, 2015](#)). The company also paid **\$1.6 million US to settle with the Federal Trade Commission(FTC)** as part of a probe into the company’s security protocols at that time ([Press, 2016](#)).

Though the identity of hackers were not known, there are some potential charges they could have faced under Canadian law which includes charges for theft, mischief to property, mischief in relation to computer data, extortion, criminal harassment, and intimidation ([Schwartz, 2015](#)).

3. Social Issues

The Ashley Madison data breach has raised concerns about various sensitive topics in society exposing millions of user's private information. Here are some of the broader social consequences that arise from data breaches:

a. Impact on society

In a society where its members are bound by certain social values and norms, many people view infidelity as moral transgression. Members in monogamous partnerships who were exposed suffered from **judgment and public mockery** on a global scale because of their privacy violations. They were made fun of on a variety of platforms, including memes, tweets, and even headlines ([Hackathorn, 2017](#)).

b. Loss of Reputation and Jobs

The hacking and exposure of Ashley Madison users' data caused a **massive reputation crisis** which was like an apocalypse for online reputation management, as it damaged the reputations of many people all at once ([Smith, 2015](#)). Many famous individual's names were exposed with some accusations proving true and others false. For instance, **Joe Biden's son** who denied having an Ashley Madison account, despite a matching email in the hack. He asserted it was created without his knowledge, stating it had severely impacted his life ([Kopan, 2015](#)). After revelation of engagement of **CEO of Avid Life Media** in extramarital affairs, despite claiming he had not, he **resigned** from his post ([Dark Reading Staff, 2015](#)).

According to the Telegraph, the data breach involved **1,716 persons at universities** and further education colleges, **124 civil officials**, **92 Ministry of Defense employees**, around **50 police officers**, **56 NHS employees**, **65 local education and school staff**, and **56 NHS workers** affecting their job and reputation ([Kirk, et al., 2015](#)).

c. Impact on Relationships and family

The breach broke trust and resulted in an immediate separation for some people while it also acted as a trigger for their **divorce**, illustrating the emotional cost of such revelations (Pagliery, 2015). But the betrayal of an affair doesn't just affect husband and wife. **Children** too are devastated by the unfaithfulness of a parent. Following the disclosure, there appeared to be a sudden rise in **divorce rates** in cities across the world, including New York and Long Island (Firm, 2015).

d. Psychological Consequences and Crimes

There are **two suicides** reported associated because of the leak of Ashley Madison customers' profiles as according to Toronto Police (Thielman, 2015). Even a beloved pastor whose name was on the list of Ashley Madison breach **committed suicide just after 6 day of data exposure** where he mentioned about his involvement on Ashley Madison (WILLIAMS, 2015).

There was also **blackmail and threats** reported after the exposure. Blackmails involved targeting Ashley Madison users demanding **\$450 or 2 Bitcoins** to avoid exposure (Gill, 2020). The **Personalized emails**, utilizing Ashley Madison breach data, include the recipient's name, bank, and intimate details such as bank account numbers and past purchases such as **"male assistance products"** which the blackmailer utilized to blackmail the individuals (Gendre, 2021).

With the data breach of Ashley Madison, the **mental, emotional, and psychological** distress its users had to face is extreme which even led to depression and loss of life as mentioned above. Post breach, the users faced the **public shaming and humiliation** in the society which impacted on their **mental health** (SAVAGE, 2015).

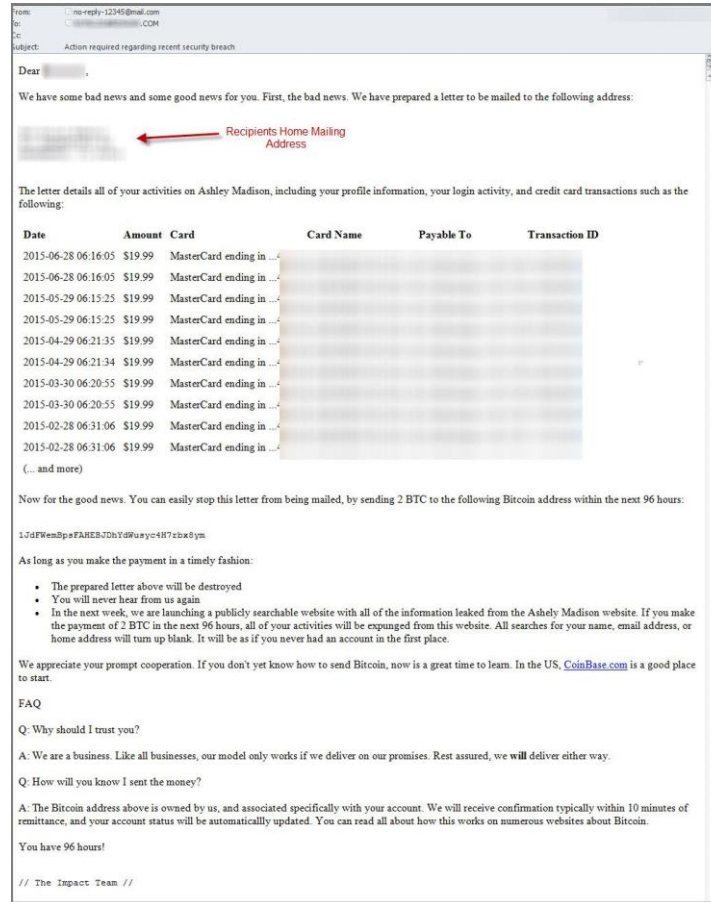


Figure 4: Blackmails and Threats after the Breach (Gill, 2020)

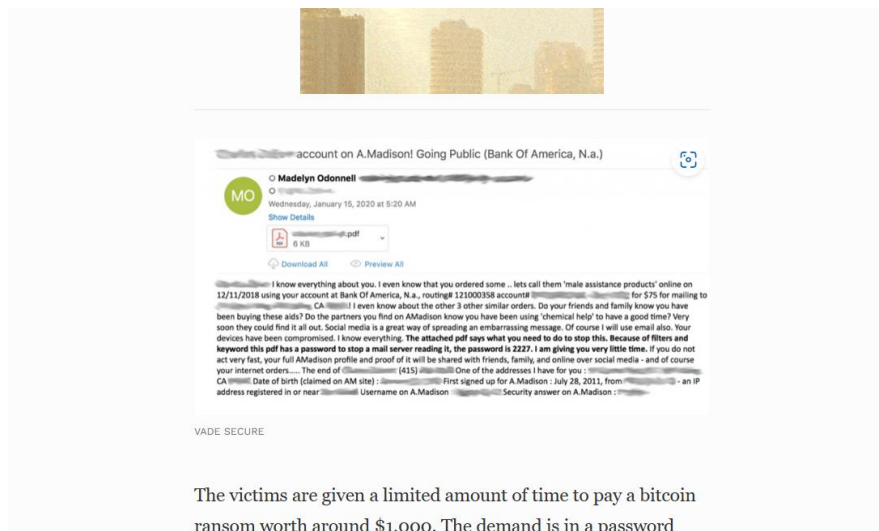


Figure 5: Blackmails and Threats after the Breach 1.0 (Gendre, 2021)

e. Gender Discrimination

The Ashley Madison hack significantly impacted **the LGBTQ community**, particularly in nations where engaging in **same-sex relationships** is illegal. Although there were less severe consequences for users in the US, their sexual orientation and other personal information was made public, which made them more open to **discrimination** (Lemberg, 2017). For example, a **gay of Saudi national** was afraid that he was going to be murdered to death after release of the data which illustrates the potentially fatal outcomes LGBTQ individuals in those areas (Gallagher, 2015).

f. Impact on Religious Faith

It was estimated that about **400 church leaders** were found on the list of Ashley Madison data breach. The involvement those pastors and leaders in the Ashley Madison scandal undermines **trust in religious institutions** and **challenges their moral authority** which lead followers to question their faith (Chan, 2015).

g. Financial loss

Due to a significant data breach, the Ashley Madison website's plans for an **IPO** were canceled. Following the data hack, the company immediately abandoned its plans for an IPO, missing out on possibilities to capitalize on the **stock market** (Bird, 2015). Additionally, regulatory fines and penalties have further strained the company's finances.

4. Ethical Issues

The Ashley Madison data breach is an ideal example of unethical behavior. Both the company and the hackers ignored fundamental ethical principles, causing harm to individuals. This incident emphasizes the crucial need for ethical considerations in data security and privacy practices. Here are some of the broader ethical consequences that arise from data breaches:

a. Dishonesty and Integrity Deficiency

Ashley Madison featured a **fake security certification** on its homepage and failed to **implement proper security measures** for user data which shows insufficient safeguard measures followed by both Ashley Madison and its parent company, Avid Life Media(ALM) (Raywood, 2016).

The scandal also exposed the use of **fake profiles**, dubbed "Ashley's Angels," which were managed by paid employees to interact with visitors. Despite the disclaimers, these profiles were intended for user entertainment which were revealed by former employees of Ashley Madison (Dewey, 2015). This unethical behavior compromises user trust and privacy. These actions primarily violate principles of **virtue ethics**.

Similarly, The **Impact Team hide their identities**, undermining principle of **honesty and transparency of virtue ethics** but compromised user privacy and trust which highlights raises ethical questions about the impact of hacking on character development and online integrity (Raicu, 2012).

b. Violations of moral justification

In the context of exposing the foolishness of millions of men and a small number of women involved in Ashley Madison, a **deontological perspective** would consider the duty to respect the privacy and confidentiality of individuals personal lives. In deontological ethics, the focus is on **moral duties and obligations**, irrespective of the consequences (Immanuel Kant, 2024). It proposes that violating **someone's privacy and confidentiality** without that person's agreement is morally wrong, even in cases where disclosing their conduct might promote a greater good. Such a duty is especially important considering all the possible harm to children and families who can end up as unintentional victims following such exposure (Kuhrt, 2015).

Regarding Ashley Madison's perspective, the investigation revealed that it was **retaining personal data even after users deleted profiles**, resulting in non-users email addresses being included in breached databases which shows insufficient safeguard measures followed by the company (Raywood, 2016).

c. Morality of facilitating infidelity

Harms caused by facilitating Infidelity such as the **breakdown of trust in relationships**, emotional distress for spouses and families, and the potential for long-term psychological consequences, outweighs any short-term happiness experienced by individuals involved in extramarital affairs (Kuhrt, 2015). This contradicts **Utilitarian ethics** which states that an action is right if it results in the happiness of the greatest number of people in a society or a group (TARDI, 2023). In this case, the consequences resulted in greater unhappiness, highlighting an inconsistency with **Utilitarian principles**. On the other hand, The Impact Team's decision to release private user information without consent demonstrates a lack of consideration for the potential **negative consequences of their actions**. While they may have sought to expose Ashley Madison's wrongdoing, the harm caused by the data breach far **outweighs any potential benefits** which contradicts **Utilitarianism**.

d. Right Ethics

Ashley Madison was **inappropriately retaining information** from users which included their personal information , their credit card details without a comprehensive information security plan which had a broad social impact violating **Right ethics** (Evans, 2016). Similarly, the hackers who called themselves as “Impact Team” **accessed data without consent** and infringe upon individuals right to privacy (Wolfe, 2015).

5. Professional Issues

The Ashley Madison data breach showed a complete violation of professional ethics and raised many professional issues. The professional issues relating to the breach are discussed below.

a. Professional Misconduct

Ashley Madison's actions do reflect a major lack of professionalism and ethics. By failing to implement security measures and maintain confidentiality, the company breached both its user's confidence and its own terms and conditions. Overall, Ashley Madison's actions constitute professional misconduct and reflect negatively on the company's dedication to ethical business practices ([Kostadinov, 2015](#)). Similarly, Impact team who misused their skills and breached the personal information of millions of users which was easily accessible on the internet lacked professionalism too ([Ward, 2015](#)).

People were even found using their cooperative email to sign in on Ashley Madison. Using corporate emails for such activities not only violates ethical standards but also demonstrates a lack of integrity and professionalism within the organization ([Raza, 2021](#)).

b. Breach of professional contracts

Ashley Madison failed to deliver on its promise of a secure and discreet platform for individuals seeking extramarital affairs. It was also engaged in fraud by establishing fake female accounts to artificially boost its user base, misinforming customers about the service's validity. This manipulation of user data and participation not only violated the terms of service agreed upon with its users, but it also damaged the platform's overall trust ([Gallagher, 2015](#)).

c. Violation of various professional code of conducts

Ashley Madison's actions violated multiple professional codes of conduct, exposing a lack of respect for ethical standards and user trust. Here's how the platform's conduct breached established professional code of conducts:

i. Violation of BCS(British Computer Society) Code of Conduct

The BCS Code of Conduct outlines key principles for IT professionals: *Public Interest, Duty to the Profession, Duty to Relevant Authority and Professional Competence and Integrity* (BCS, The Chartered Institute for IT, 2022). Ashley Madison violated the **BCS Code of Conduct** multiple times. First, they ignored public health and fairness by **promoting extra marital affairs** while failing to **protect user privacy**. Second, they were **dishonest** by creating **fake profiles** to deceive users. Third, they failed to follow **data security regulations**, which are critical for establishing confidence. Finally, Prioritizing profit over ethics damages **professional standards**.

ii. Violation of ACM(Association of Computing Machinery) Code of Conduct

The ACM Code of Ethics provides essential guidelines for **computing professionals**, emphasizing **leadership commitment** and adherence to ethical principles. It extends beyond computing to encompass broader ethical concepts, addressing conflicts through **fundamental analysis rather than strict legal interpretation** (Baase, 2012).

The ACM Code of Ethics advocates for *societal contribution, harm prevention, and honest and fair behavior* promoting quality work, continuous improvement, and respect for norms and privacy (ACM, 2018). Ashley Madison, by facilitating **extramarital affairs** undermines societal well-being by eroding trust and potentially harming relationships. Similarly, the Impact Team's **unauthorized access** to private user data violates ethical principles, causing **psychological distress and harm** to individuals. This breaches the **principle of avoiding harm** because of the data breach.

iii. Violation of IEEE(Institute of Electrical and Electronics Engineers) Code of Conduct

The IEEE Code of Conduct emphasizes *respect, fairness, and integrity*. *It prohibits harassment, discrimination, and retaliation* (IEEE, 2020). Ashley Madison and the Impact Team's actions in committing the data breach and disclosing sensitive user information obviously breached the fundamental principles outlined in the IEEE Code of Conduct.

The Impact Team's breach of Ashley Madison's database compromised user privacy and fairness, lead to severe actions, and broke laws and policies. They caused harm by revealing sensitive data, which violated the IEEE Code of Conduct's principle of non-retaliation. Furthermore, their improper access and disclosure of user data violated laws and the IEEE policy on confidentiality and privacy rights.

6. Conclusion

Following the incident, the Ashley Madison affair initiated by “The Impact Team” revealed the complex web of human desire and made people reconsider their actions online. The unauthorized use of customer’s information not only damaged the **company’s reputation** but caused major **criticism** in people’s lives. It sparked discussions on **moral and religious principles**, as well as **ethical considerations** in technology and privacy which acted as an upsetting reminder of the importance of data protection and the long-term consequences of cyber breaches.

The Ashley Madison scandal is a **complex tangle of challenges** that has impacted a lot of people. From the company itself to its users, their partners, broader society, and even the workers at Ashley Madison, all are recognized as **tackling challenges** with misuse of data, breach of privacy, reliability loss, transparency, and damage to reputation which has left a significant and **wide-ranging impact** including psychological trouble for affected people, legal trouble to the company prompting a societal reconsideration of relationships. While the scandal has also **benefitted** some parties for **short term** such as hacker getting recognition from public, lawyers getting limelight and company getting unintentionally promoted to the users who have never heard of it, the negative consequences and harm is far-reaching.

Ashley Madison had several choices for responding to the hack to **minimize the harm** and restore trust. They had the opportunity to enhance the cybersecurity measures, quickly inform users about the breach, offer support services like credit monitoring and counseling, work with law enforcement to investigate and enforce the incident, and put in place stronger security procedures to stop similar ones in the future.

In analyzing the Ashley Madison situation, the CEO or board should put **everyone’s welfare first**. Upholding the **rights to privacy** and fair treatment for everyone involved is essential. In the decision-making process, it’s crucial to implement **preventive measures** to enhance security and transparency, preventing data breaches like performing steps to increase the clarity of the agreement’s conditions, implement two-step authentication, offering comprehensive data usage information, and initiating interactions with cybersecurity agencies. This comprehensive approach ensures that ethical considerations, such as respecting user privacy and promoting transparency, are at the forefront of decision-making.

In conclusion, the most efficient course of action for preventing data breaches, ensuring transparency, and reestablishing public trust is to give priority to **cybersecurity improvements**. This strategy entails working with relevant authorities, establishing strong security measures in place, and quickly fixing weaknesses. Ashley Madison tends to successfully handle these issues and earn back user trust by prioritizing user privacy, following the ethical codes of conduct, and making sensible choices. As such, this action is prioritized over other alternative approaches to address these issues.

7. References

ACM, 2018. *Code of Ethics*. [Online]
Available at: <https://www.acm.org/code-of-ethics>
[Accessed 24 April 2024].

AGARWAL, O., 2023. *Who owns Ashley Madison? Hulu's 'The Ashley Madison Affair' exposes controversial history of dating site - MEAWW*. [Online]
Available at: <https://meaww.com/who-owns-ashley-madison-hulus-the-ashley-madison-affair-exposes-controversial-history-of-dating-site>
[Accessed 16 April 2024].

Baase, S., 2012. ACM Code of Ethics and Professional Conduct. In: T. J. C. S. J. H. J. B. Marcia Horton, ed. *A Gift of Fire*. New York: Pearson, NY, pp. 447-454.

BCS, The Chartered Institute for IT, 2022. *BCS Code of Conduct for members - Ethics for IT professionals* / *BCS*. [Online]
Available at: <https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf>
[Accessed 24 April 2024].

Bird, M., 2015. *How Close Ashley Madison Came to an IPO*. [Online]
Available at: <https://www.businessinsider.com/how-close-ashley-madison-came-to-an-ipo-2015-8>
[Accessed 24 April 2024].

CBC News, 2015. *Ashley Madison owner to pay up to \$11.2M to settle U.S. class action lawsuits* / *CBC News*. [Online]
Available at: <https://www.cbc.ca/news/business/ashley-madison-ruby-lawsuits-1.4208792>
[Accessed 22 April 2024].

Chan, E., 2015. *Christian Leaders found on Ashley Madison – Calvin University Chimes*. [Online]
Available at: <https://calvinchimes.org/2015/09/11/christian-leaders-found-on-ashley-madison/>
[Accessed 24 April 2024].

Clifford Chance, 2016. *Caught in the (Privacy) Act – The Ashley Madison data breach report*, Sydney: Clifford Chance.

Cox, J., 2015. *Ashley Madison Hackers Speak Out: 'Nobody Was Watching'*. [Online] Available at: <https://www.vice.com/en/article/bmjqyz/ashley-madison-hackers-speak-out-nobody-was-watching> [Accessed 18 April 2024].

Dark Reading Staff, 2015. *Ashley Madison CEO Resigns*. [Online] Available at: <https://www.darkreading.com/cyberattacks-data-breaches/ashley-madison-ceo-resigns> [Accessed 19 April 2024].

Dewey, C., 2015. *Ashley Madison faked female profiles to lure men in, hacked data suggest - The Washington Post*. [Online] Available at: <https://www.washingtonpost.com/news/the-intersect/wp/2015/08/25/ashley-madison-faked-female-profiles-to-lure-men-in-hacked-data-suggest/> [Accessed 19 April 2024].

Evans, P., 2016. *AshleyMadison security protocols violated privacy laws, watchdog says | CBC News*. [Online] Available at: <https://www.cbc.ca/news/business/ashley-madison-privacy-security-1.3732413> [Accessed 19 April 2024].

Firm, R. L., 2015. *Does the Ashley Madison Account Hack Affect Divorce in New York?*. [Online] Available at: <https://www.rubenfelddivorce.com/blog/2015/august/ashley-madison-hack-and-how-it-affects-divorce/> [Accessed 24 April 2024].

Gallagher, P., 2015. *Ashley Madison hack: Just three in every 10,000 female accounts on infidelity website are real | The Independent | The Independent*. [Online] Available at: <https://www.independent.co.uk/tech/ashley-madison-hack-just-three-in-every-10-000-female-accounts-on-infidelity-website-are-real-10475310.html> [Accessed 24 April 2024].

Gallagher, P., 2015. *Ashley Madison hack: Leaking personal email addresses puts gay lives at risk around the world* / *The Independent* / *The Independent*. [Online] Available at: <https://www.independent.co.uk/tech/ashley-madison-hack-leaking-personal-email-addresses-puts-gay-lives-at-risk-around-the-world-10464546.html>

[Accessed 24 April 2024].

Gendre, A., 2021. *Ashley Madison Data Breach: 5 Years Later, New Extortion Scam*. [Online] Available at: <https://www.vadesecure.com/en/blog/ashley-madison-data-breach-fuels-new-extortion-scam>

[Accessed 24 April 2024].

Gill, T., 2020. *Blackmail Messages: Ashley Madison Users Become Targets* / *AppRiver*. [Online] Available at: <https://appriver.com/blog/201508blackmail-messages-ashley-madison-users-become-targets>

[Accessed 24 April 2024].

Hackathorn, J., 2017. From fear and guilt: negative perceptions of Ashley Madison users. *Psychology* & *Sexuality*, 8(<https://www.tandfonline.com/doi/full/10.1080/19419899.2017.1316767>), pp. 41-54.

IEEE, 2020. *IEEE - IEEE Code of Ethics*. [Online] Available at: <https://www.ieee.org/about/corporate/governance/p7-8.html>

[Accessed 24 April 2024].

Immanuel Kant, H. P., 2024. *Deontological ethics* / *Definition, Meaning, Examples, & Facts* / *Britannica*. [Online]

Available at: <https://www.britannica.com/topic/deontological-ethics>

[Accessed 19 April 2024].

Jones, S. N., 2017. Having An Affair May Shorten Your Life: The. *Reading Room*, 33(2), p. 30.

Kirk, A., Gordonrayner & Ward, V., 2015. *Ashley Madison data dump exposes hundreds of public servants in sensitive positions*. [Online]

Available at: <https://www.telegraph.co.uk/news/worldnews/northamerica/usa/11813318/Ashley->

Madison-data-dump-exposes-hundreds-of-public-servants-in-sensitive-positions.html

[Accessed 24 April 2024].

Kopan, T., 2015. *Hunter Biden denies link to Ashley Madison* / *CNN Politics*. [Online]

Available at: <https://edition.cnn.com/2015/08/25/politics/hunter-biden-ashley-madison-denial/>

[Accessed 19 April 2024].

Kostadinov, D., 2015. *Ashley Madison Revisited: Legal, Business and Security Repercussions* / *Infosec*. [Online]

Available at: <https://www.infosecinstitute.com/resources/news/ashley-madison-revisited-legal-business-and-security-repercussions/>

[Accessed 24 April 2024].

KrebsOnSecurity, 2015. *AshleyMadison: \$500K Bounty for Hackers – Krebs on Security*.

[Online]

Available at: <https://krebsonsecurity.com/2015/08/ashleymadison-500k-bounty-for-hackers/comment-page-1/>

[Accessed 16 April 2024].

Kuhrt, J., 2015. *Illegal, but moral? Were the Impact Team right to hack Ashley Madison? – Grace + Truth*. [Online]

Available at: <https://gracetruth.blog/2015/08/28/illegal-but-moral-were-the-impact-group-right-to-hack-ashley-madison/>

[Accessed 19 April 2024].

Lemberg, A., 2017. Hackers Made Me Lose My Job!: Health Data Privacy and Its Potentially Devastating Effect on the LGBTQ Population. *Golden Gate University Law Review*, 47(2), pp. 4-10.

Lord, N., 2017. *A Timeline of the Ashley Madison Hack*. [Online]

Available at: <https://www.digitalguardian.com/blog/timeline-ashley-madison-hack>

[Accessed 12 April 2024].

Megan, G., 2015. *Paying \$20 to delete your Ashley Madison profile was probably a bad idea* / *Ars Technica*. [Online]

Available at: <https://arstechnica.com/information-technology/2015/07/cheaters-hook-up-site-ashley-madison-makes-account-deletion-confusing/>

[Accessed 23 April 2024].

MILLER, A., 2023. *Ashley Madison Reviews - Does It Work in 2023? What I Learned on This Dating Site* / *Miami Herald*. [Online]

Available at: <https://www.miamiherald.com/indulge/article271143687.html>

[Accessed 13 April 2024].

O'Brien, C., 2016. *Ashley Madison's parent company rebrands as Ruby, drops infamous 'Have an affair' tagline* / *VentureBeat*. [Online]

Available at: <https://venturebeat.com/business/ashley-madisons-parent-company-rebrands-as-ruby-drops-infamous-have-an-affair-tagline/>

[Accessed 16 April 2024].

Office of the Privacy Commissioner of Canada, 2016. *News Release: Ashley Madison investigation finds security measures lacking; fictitious security trustmark was 'deceptive' - August 23, 2016 - Office of the Privacy Commissioner of Canada*. [Online]

Available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c_160823/

[Accessed 16 April 2024].

Orchard, T., 2019. Dating Apps. In: A. D. Lykins, ed. *Encyclopedia of Sexuality and Gender*. Switzerland: Springer, Cham, pp. 112-113.

Pagliery, J., 2015. *The Ashley Madison hack ruined my life*. [Online]

Available at: [by Jose Pagliery](#)

[Accessed 24 April 2024].

Press, T. C., 2016. *Ashley Madison parent company Ruby pays \$1.6M to settle FTC probe* / *CBC News*. [Online]

Available at: <https://www.cbc.ca/news/business/ashley-madison-ruby-ftvc-fine-1.3896283>

[Accessed 22 April 2024].

Raicu, I., 2012. *Unavoidable Ethical Questions About... Hacking* - *Markkula Center for Applied Ethics*. [Online]

Available at: <https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unavoidable-ethical-questions-about-hacking/>

[Accessed 19 April 2024].

Raywood, D., 2016. *Ashley Madison had major failures on user security - Infosecurity Magazine*. [Online]

Available at: <https://www.infosecurity-magazine.com/news/ashley-madison-failed/>

[Accessed 18 April 2024].

Raza, S., 2021. *Corporate Culture: Ashley Madison And Corporate Fraud*. [Online]

Available at: <https://www.valuewalk.com/corporate-culture-fraud-signs/>

[Accessed 24 April 2024].

SAVAGE, D., 2015. *Letters From Ashley Madison Users - The Stranger*. [Online]

Available at: <https://www.thestranger.com/news/2015/08/25/22756209/letters-from-ashley-madison-users>

[Accessed 24 April 2024].

Schwartz, D., 2015. *Ashley Madison hackers Impact Team could face long list of charges / CBC News*. [Online]

Available at: <https://www.cbc.ca/news/science/ashley-madison-hackers-impact-team-could-face-long-list-of-charges-1.3203279>

[Accessed 18 April 2024].

Smith, C. S., 2015. *For Ashley Madison Users, What's Next? Reputation Apocalypse, Phase 2*. [Online]

Available at: <https://martech.org/ashley-madison-users-whats-next-reputation-apocalypse-phase-2/#.VqKc9eNwqHg.email>

[Accessed 19 April 2024].

TARDI, C., 2023. *Utilitarianism: What It Is, Founders, and Main Principles*. [Online]

Available at: <https://www.investopedia.com/terms/u/utilitarianism.asp>

[Accessed 19 April 2024].

Thielman, S., 2015. *Toronto police report two suicides associated with Ashley Madison hack / Canada* / *The Guardian*. [Online]
Available at: <https://www.theguardian.com/world/2015/aug/24/toronto-suicides-ashley-madison-hack>

[Accessed 24 April 2024].

Trendmicro, 2018. *Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes* - *Security News*. [Online]
Available at: <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101>

[Accessed 13 April 2024].

Ward, M., 2015. *Ashley Madison: Who are the hackers behind the attack? - BBC News*. [Online]
Available at: <https://www.bbc.com/news/technology-34002053>

[Accessed 24 April 2024].

WILLIAMS, M. E., 2015. *An Ashley Madison suicide: It shouldn't take a tragedy to end the gleeful "cheating dirtbags" schadenfreude* / *Salon.com*. [Online]
Available at:
https://www.salon.com/2015/09/09/an_ashley_madison_suicide_it_shouldnt_take_a_tragedy_to_end_the_gleeful_cheating_dirtbags_schadenfreude/

[Accessed 24 April 2024].

Wolfe, N. A., 2015. Using the Computer Fraud and Abuse Act to Secure Public Data Exclusivi. *Northwestern Journal of Technology and Intellectual Property*, 13(3), p. 21.