AI, DATA, AND TECHNOLOGY

Berkay Dur

Ethics, Regulation and Law in Advanced Digital Information Processing and Decision Making

ECS7025P

Artificial Intelligence MSc

Submission Date: 11/05/2023

Word Count: 4637

Table of Contents

List of Abbreviations

AI – Artificial Intelligence

AWS – Autonomous Weapons Systems

NGO – Non-Governmental Organization

UN – United Nations

IHL – International Humanitarian Law

GGE – Government of Governmental Experts

CCW – Conference of Certain Conventional Weapons

UAV – Unmanned Aerial Vehicle

USV – Unmanned Surface Vehicle

CAGR – Compound Annual Growth Rate

POW – Prisoners of War

XAI – Explainable AI

ICO – Information Commissioner’s Office

CERT – Computer Emergency Readiness Team

GAO – Government Accountability Office

SME – Small and medium-sizes Enterprises

NLP – Natural Language Processing

FBI – Federal Bureau of Investigation

Abstract

This report explores the ethical implications of Autonomous Weapons Systems through international law, analyses the Equifax data breach within the framework of UK GDPR, and examines the role of new technologies, like AI, in industries like finance and music streaming. It emphasizes the need for international collaboration, robust data privacy protection, responsible AI deployment, and increased security measures. The report highlights the importance of ethical frameworks, legal regulations, and awareness in mitigating risks and maximising the benefits of technological advancements across diverse domains.

Section A: Autonomous Weapons Systems

Introduction

"Artificial intelligence is the future not only of Russia but all of mankind… Whoever becomes the leader in this sphere will become the ruler of the world" (Gigova, 2017).

This quote by Vladimir Putin summarises the sentiment of militaries around the world regarding the development and deployment of AI (Heikkilä, 2022). With AI development in the military outpacing laws and regulations, it has the potential to cause great harm and revolutionize warfare through the deployment of AWS. The NGO 'Stop Killer Robots', describes AWS as being able to "select and attack targets" and "challenge human control over the use of force." (StopKillerRobots, n.d.). While AWS can enhance military capabilities and provide strategic advantages (Etzioni and Etzioni, 2018), its ethical implications warrant critical examination.

This report aims to explore the ethics surrounding AWS by analyzing its potential benefits and drawbacks, as well as examining the current legal and ethical frameworks governing its development and use. The author acknowledges that AI presents both opportunities and challenges and emphasizes the importance of addressing ethical concerns to minimize harm, particularly in the context of AWS, which could pose a significant risk to non-combatants.

Definitions and Capabilities

AWS is a contentious issue in international law, as will be explored later, to the extent that it does not have a formal definition in the UN and the IHL. This report uses the following definition as submitted by the State of Palestine at the meeting of the GGE at the CCW as it most cohesively encapsulates the capabilities of AWS: "**Autonomous Weapons Systems** (AWS) are systems that, upon activation by a human user(s), use the processing of sensor data to select and engage a target(s) with force without human intervention." (State of Palestine, 2023). The author appreciates that there exist different definitions in the literature, mainly defining AWS with a degree of autonomy, with one such definition using the phrases "human in the loop" and "human out of the loop", but this report chooses to focus solely on AWS as defined above with regards to its challenges to ethics, law, and morality.

To date, several militaries have reported investment and development into AWS (Kayser, 2022), creating an international arms race, with the first reported case of an AWS attacking a human target coming from Libya in 2020 (Choudhury, 2021). AWS are currently confined to drones but militaries are expanding their usage to other weapons systems, such as UAVs and USVs, at an alarming pace (Kayser, 2022). The global AWS market is expected to grow at a CAGR of 10.4%, and as such is expected to reach a value of $19.75 billion in 2026 (BusinessWire, 2022) with an increasing number of companies developing AWS (Kayser, 2022).

Ethical benefits of AWS

Integrating AWS alongside human force or as a replacement in military operations presents potential ethical benefits. The following non-exhaustive list highlights some of these advantages:

1. **Reducing harm to military personnel.** AWS can be utilized in situations that are inherently dangerous for humans which could cause immediate harm, lead to long-term health complications, and lasting psychological effects. For instance, AWS could be deployed in areas of high radiation, where human involvement would carry substantial risk.

2. **The ability to act conservatively.** Unlike humans, who may exhibit a "fight or flight" response in stressful conflict situations causing them to act with impaired judgment, AWS will act objectively and can be programmed to strike only when target identification surpasses

a certain threshold. As argued by Arkin this eliminates the potential for a ‘shoot first, ask questions later approach, which could lead to ethical violations (Arkin, 2010).

3. **Objective reporting of ethical violations.** Loyalty and camaraderie might deter soldiers from reporting ethical violations committed by their peers. As per Figure 1, only 40% of the marines and 55% of soldiers surveyed would agree or strongly agree with reporting a unit member for injuring or killing an innocent non-combatant. In contrast, AWS can offer a more objective perspective, ensuring that such incidents are properly reported.

4. **Reduction in ethical violations.** Soldiers are in positions of power over POWS and non-combatants and as such they must comply with the IHL. However, a mob-like mentality and heightened emotions could lead to ethical violations. This is evidenced by Figure 2, which states that soldiers and marines with high levels of anger were twice as likely to commit ethical violations, such as physically hitting/kicking non-combatants when it was not necessary than those who have low levels of anger (Surgeon General, 2006). AWS could act as a deterrence to soldiers purposefully violating the IHL.

5. **In-built compliance with IHL.** Figure 3 shows that around 80% of soldiers and marines agree or strongly agree that they have received adequate training in how to deal with non-combatants. Yet, just over a quarter agree or strongly agree that they have encountered ethical situations in which they did not know how to respond. AWS can be programmed to strictly adhere to the principles of the IHL and can navigate such situations with certainty.

6. **Increased precision, accuracy, and response time.** AI is already being used to enhance the targeting of weapons systems due to its superior precision, accuracy, and response time. While humans currently ‘pull the trigger,’ AWS could further reduce the likelihood of ethical violations resulting from uncertainties and errors.

7. **Overcoming ‘scenario fulfilment’.** Military personnel may experience a phenomenon known as ‘Scenario Fulfilment,’ potentially leading to ethical violations. AWS, not being subject to such psychological factors, can help mitigate the risks associated with the phenomenon (Arkin, 2010).

In summary, the deployment of AWS in the military has the potential to offer several ethical benefits ranging from reducing harm to military personnel and enhancing compliance with IHL, to ensuring impartiality and overcoming human limitations in decision-making.

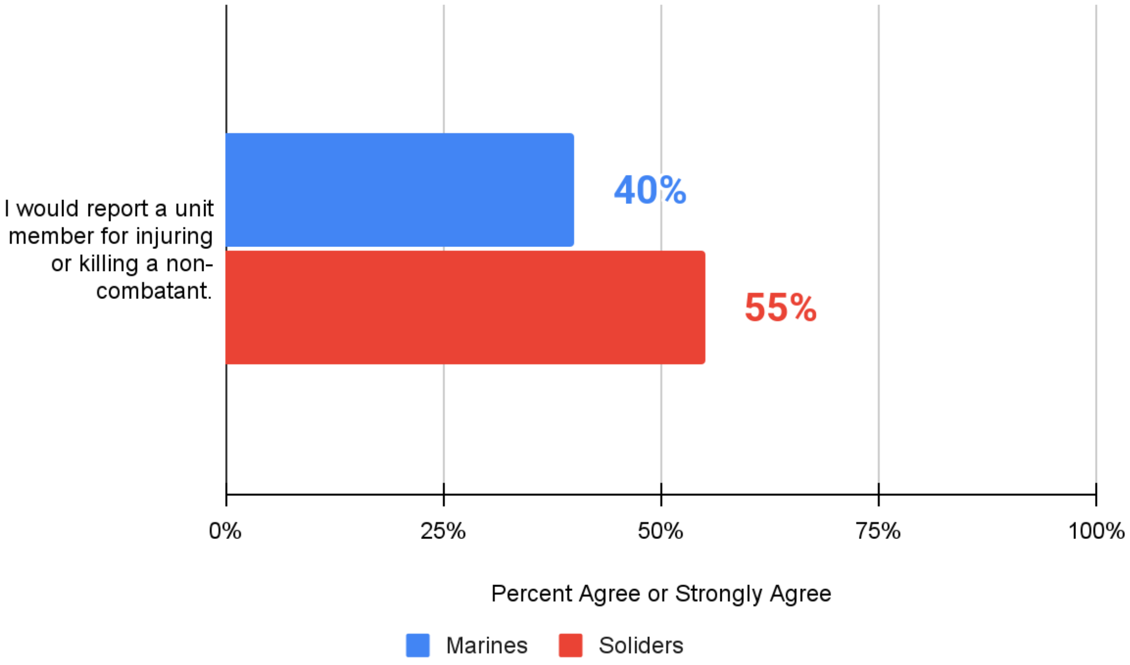


Figure 1. Percentage of soldiers and marines who would report a unit member for injuring or killing an innocent non-combatant (Surgeon General, 2006).

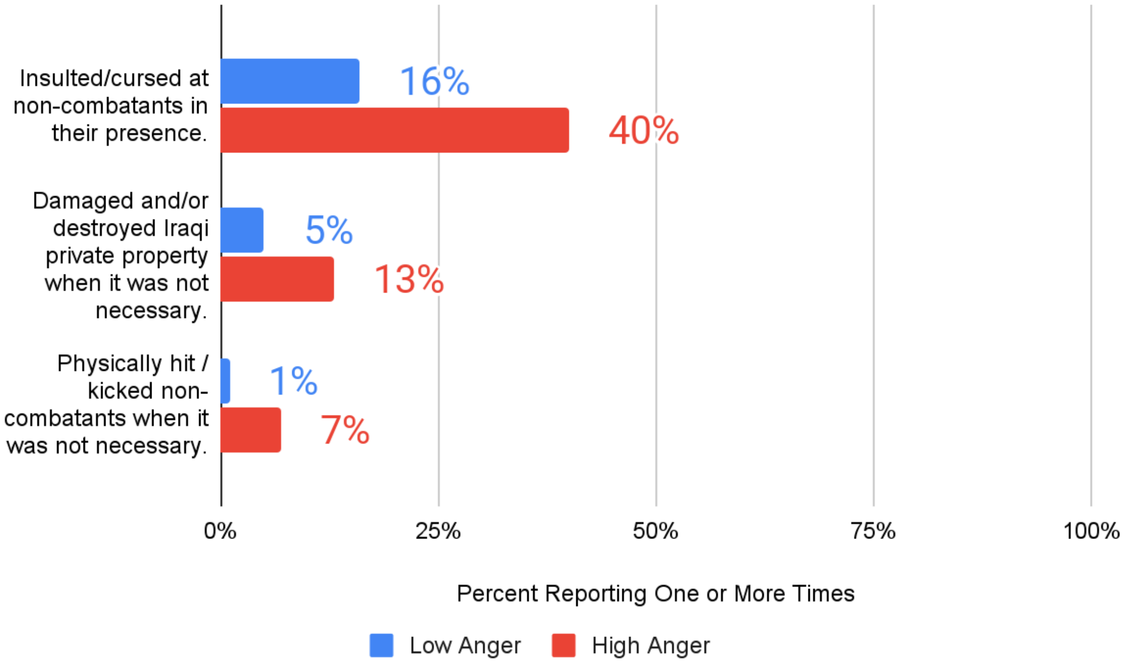


Figure 2. The effect of anger on the mistreatment of Iraqi non-combatants (Surgeon General, 2006).

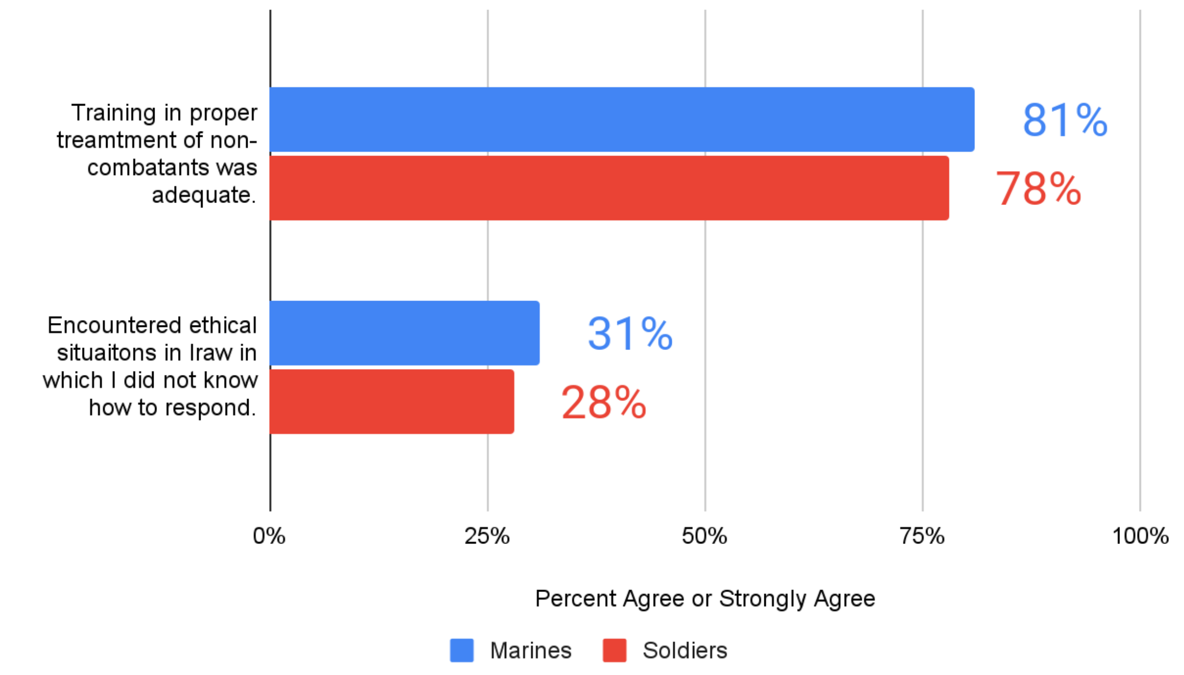


Figure 3. Soldier and Marine attitudes towards battlefield ethics training (Surgeon General, 2006).

Ethical Issues of AWS

The following is a non-exhaustive list of ethical issues regarding the development and deployment of AWS:

1. **Accountability.** As will be explored later, accountability for war crimes is a central part of the IHL to ensure that individuals are held accountable for their actions. Autonomous AI raises fundamental questions about accountability in law. For example, if an AWS commits a war crime should any human be to blame? Should we blame the commander who approved its usage, even though they did not decide on its actions? Or should we blame the programmer? Or perhaps the person who collected the data? Collaboration is needed between governments to ensure a sufficient legal framework is in place to address this ethical dilemma.

2. **Answerability.** Deep neural networks are inherently unexplainable. This again raises fundamental questions about the law, in this case, answerability. A lack of explainability makes it difficult to determine if the actions of an AWS are justified which in turn makes it difficult to determine if IHL was violated and if so, why it was violated. A potential solution to this problem is XAI.

3. **Creating an empathy gap.** The use of AWS could create an empathy gap. By eliminating the human variable from war, leaders will be more daring with entering conflicts having eliminated the risk of death to their troops. This could result in the death and displacement of non-combatants.

4. **Bias.** Whilst AWS could be implemented for its potential for objectivity, biased AWS raises fundamental questions about equality and fairness. In conflict, the IHL must be upheld with rule 88 being concerned with the non-biased application of IHL based on the following factors ‘race, colour, sex, language, religion or belief, political or other opinion, national or social origin, wealth, birth or other status, or on any other similar criteria’ (IHL, n.d.). A biased AWS could target particular groups based on any other factors and cause

disproportionate harm to that group. For example, the AWS could misinterpret cultural nuances leading it to cause harm to particular cultural groups.

5. **Unpredictability.** AWS trained using deep neural networks have the potential to behave erratically, producing disastrous results. Conflicts zones are complex and dynamic which could lead the AWS to behave in unpredictable ways. This could lead to IHL violations and cause harm to non-combatants.

The deployment of AWS raises ethical issues surrounding accountability, answerability, empathy gap, bias, and unpredictability, all of which could lead to IHL violations and disproportionate harm to certain groups.

The above literature has not carried out a critical, balanced evaluation of the ethical considerations of AWS. The author of this report believes that AWS have the potential to transform conflict into a more ethical landscape and provide wider benefits to society. However, with unregulated development and deployment, it will continue to challenge the foundations of the ethical frameworks and laws that protect non-combatants from conflict. Going forward, representatives must consider these challenges to ensure that innovation does not cause harm and regulations do not inhibit innovation.

Laws and Regulations

Despite the effort of many countries and NGOs, there is still no legal definition or legislation on AWS in international law. The existing legal framework of the IHL does not provide any specifics on AWS but states that all weapons must adhere to the legislation. The problem with the legislation is that it does not address any of the fundamental ethical issues that AWS raises.

The CCW has opened talks on AWS since the 2010s but to no avail. Preceding the most recent meeting of the GGE at the CCW in 2023, a communique from 33 Latin American and Caribbean countries called for ‘the urgent negotiation of an international legally binding instrument on autonomy in weapons systems’ (UNA, 2023). At the meeting, there were a total of 5 proposed frameworks on the governance of AWS (Reaching Critical Will, 2023). It seems that states have differing views on the regulations of AWS. The group led by the US proposed a regulation on AWS that does not comply with the current IHL but continued to ‘shy away from commitment to new legally binding rules’ (Stop Killer Robots, 2023). The proposals by Austria and the State of Palestine call for further international regulation as necessary to ensure ‘meaningful human control over autonomous weapons systems and the use of force as well as to protect human dignity’ (Austria, 2023) as it raises fundamental ethical issues. Both these proposals call for an outright ban on AWS that ‘select and engage persons’ (Austria, 2023). The proposal by the Russian Federation ‘falls drastically short of the international legally binding instrument that is urgently required’ (Stop Killer Robots, 2023). These talks highlight the differing views of states to regulate AWS.

Conclusion

International laws relating to AWS are lacking. This is a common pattern in the AI sphere as governments struggle to regulate innovation. The ethical issues surrounding AWS are complex and must be addressed to prevent harm to non-combatants and ensure compliance with the IHL. While there are potential ethical benefits to using AWS in military operations, these benefits must be balanced against the risks and challenges that such systems pose. To ensure the responsible development and deployment of AWS, international collaboration, and agreement on legal and ethical frameworks are essential. With the increasing investment and development of AWS, the need for international regulation becomes more urgent. It is crucial for the international community to reach a consensus on the ethical and legal aspects of AWS, to prevent an escalation of conflicts and to safeguard the rights of non-combatants in future armed conflicts.

Section B

Introduction

With the rapid development of AI, the role of cybersecurity is becoming ever more important with 83% of organizations reporting having had more than one data breach with the average data breach in 2022 costing approximately $4.35 million (IBM, 2022). Companies are increasingly mining the personal data of individuals and without proper investment in cybersecurity, individuals fall victim to personal data leaks. Government regulations exist to protect the right to data privacy for individuals. This report will give an insight into the Equifax 2017 data breach from the perspective of UK GDPR.

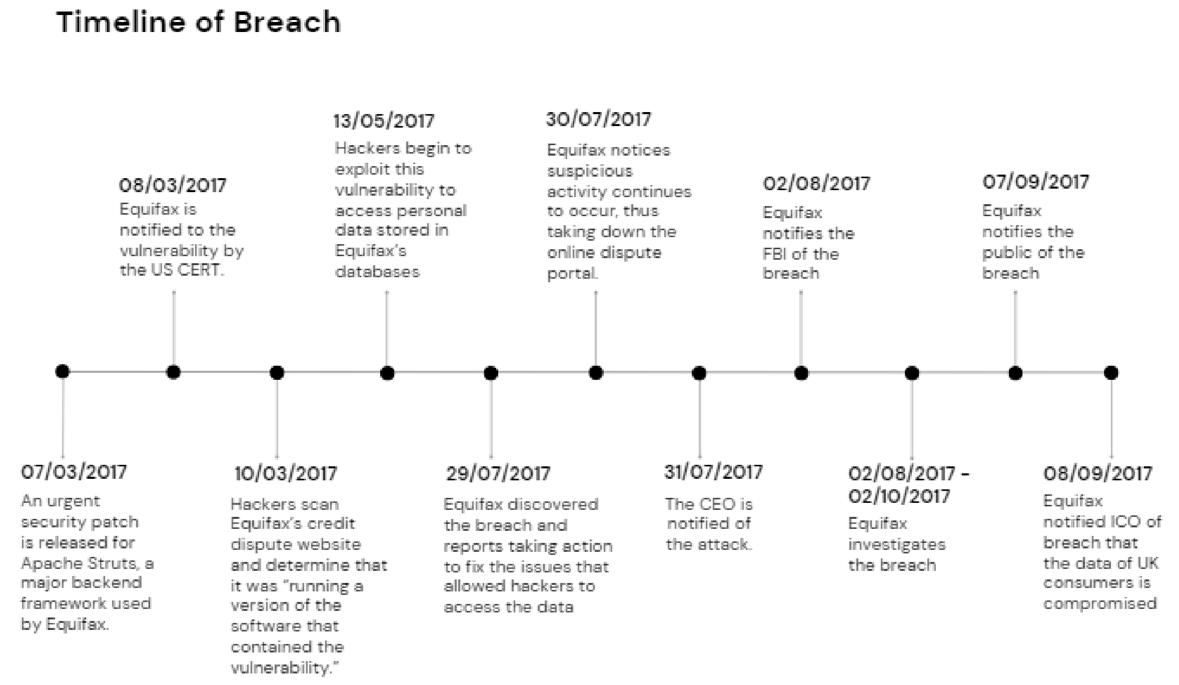
What is a Data Breach?

In the existing literature, a data breach is generally defined as 'any security incident in which unauthorized parties gain access to sensitive data or confidential information, including personal data (Social Security Number, Banking Account Number, Healthcare data) or corporate data (customer data, intellectual property, financial information)' (IBM, n.d.). This is a very general definition that encompasses all types of breaches. Although this may be a useful definition for evaluating the potential loss for a company, the UK GDPR specifically focuses on personal data breaches to ensure the protection of personal data, the privacy of individuals, and just punishment in cases of personal data breaches. UK GDPR defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (UK GDPR).

The author of this report believes that individuals are the sole victims in cases of personal data breaches, with these breaches having a range of effects on individuals, including 'emotional distress, and physical and material damage' (ICO, 2019). To make up for lost revenue after data breaches, IBM reports that 60% of organizations increase prices (IBM, 2022), thus passing the financial burden to already victimized consumers.

Equifax Data Breach 2017

Equifax describes itself as a 'global data, analytic, and technology company' (Equifax, 2023). It is one of the biggest consumer credit reference agencies in the UK and USA (Equifax, n.d.), and as a result, has access to the personal data of millions of people. In 2017, Equifax suffered a data breach that compromised the personal data of 147.9 million Americans (epic, 2021), 15.2 million British citizens (ICO V. Equifax Ltd, [2018]), and about 19,000 Canadians. Equifax agreed to a settlement of $575 million for damages to affected individuals in the US and to make organizational changes to avoid similar breaches in the future (Federal Trade Commission, 2019). The UK ICO also took the necessary action under UK law at the time, which was the DPA 1998, leading to a fine of only £500,000 (ICO V. Equifax Ltd, [2018]). This report will examine the breach under the UK GDPR, which is implemented through the DPA 2018.



Timeline of Breach

07/03/2017 An urgent security patch is released for Apache Struts, a major backend framework used by Equifax.

08/03/2017 Equifax is notified to the vulnerability by the US CERT.

10/03/2017 Hackers scan Equifax's credit dispute website and determine that it was "running a version of the software that contained the vulnerability."

13/05/2017 Hackers begin to exploit this vulnerability to access personal data stored in Equifax's databases

29/07/2017 Equifax discovered the breach and reports taking action to fix the issues that allowed hackers to access the data

30/07/2017 Equifax notices suspicious activity continues to occur, thus taking down the online dispute portal.

31/07/2017 The CEO is notified of the attack.

02/08/2017 Equifax notifies the FBI of the breach

02/08/2017 - 02/10/2017 Equifax investigates the breach

07/09/2017 Equifax notifies the public of the breach

08/09/2017 Equifax notified ICO of breach that the data of UK consumers is compromised

Figure 4. Timeline of the main events of the Equifax Data Breach (ICO V. Equifax Ltd, [2018]), (Federal Trade Commission, 2019).

The following are the key security factors that Equifax believes led to the breach (Federal Trade Commission, 2019):

Identification. Equifax states that the 'Apache Struts vulnerability was not properly identified as being present on the online dispute portal' (Federal Trade Commission, 2019). The US-CERT notified Equifax that the security patch requires 'immediate action' due to being a 'critical vulnerability' (ICO V. Equifax Ltd, [2018]).

Detection. Equifax was quick to detect the breach at 77 days, which is 250% faster than the mean time in 2017 (IBM, 2022). They state that their inability to detect the breach was due to an out-of-date certificate which meant that they could no longer detect the malicious traffic through their network. It can also be said that Equifax clearly did not have sufficient safeguarding or monitoring in place for the detection of anomalous patterns within the network. Another example of this is the fact that the attackers were able to execute an abnormal number of queries without being detected. Equifax acknowledged that this is another important factor (Federal Trade Commission, 2019).

Segmentation. As Equifax states, the individual databases were not segmented, which means that the attackers were able to access additional databases beyond the ones related to the online dispute portal. This meant that with the expired certificate, the attackers were easily able to access a lot of personal data (Federal Trade Commission, 2019).

Data Governance. Once in the network, the attackers were able to gain access to an unencrypted file containing plaintext passwords. By not encrypting this personal data and setting limits on access to sensitive information, the attackers were able to access additional databases containing personal data (Federal Trade Commission, 2019).

Violations of UK GDPR

In the following section, Equifax Ltd, the UK entity of Equifax, is the Controller, and Equifax Inc, the US entity of Equifax, is the Processor.

Both the GAO and ICO found that there was a serious lack of proper security implementation that allowed the attackers to cause the harm they did, the security issues are as explained above.

Article 5 of the UK GDPR is the principle relating to the processing of personal data. 5.2 states that the controller is responsible for, and must be able to demonstrate compliance with 5.1, accountability. Equifax Ltd's lack of auditing and its inability to outline 'adequate safeguards / security requirements' in the contractual agreement with Equifax Inc means that Equifax Ltd is in breach of points e and f, 'storage limitation' and 'integrity and confidentiality, respectively (ICO V. Equifax Ltd, [2018]).

Article 24 pertains to the 'Responsibility of the Controller'. Equifax Ltd is in clear violation of Section 24.1 due to their inability to identify the 'risks' and implement 'appropriate technical or organisational measures' from the lack of auditing and scrutiny that Equifax Inc received from Equifax Ltd. Equifax Ltd is also in violation of 24.2 due to a lack of 'appropriate data protection policies'. This is evidenced by the lacking contractual agreement between Equifax Ltd and Equifax Inc, see the previous paragraph.

Equifax Ltd is also in violation of **Article 25**, 'Data protection by design and by default'. 25.1 is violated as Equifax Ltd, the controller, was unable to 'implement appropriate technical and organisational measures [...] in an effective manner' and to integrate 'necessary safeguards' (UK GDPR). Once again, the lacking contractual agreement between Equifax Ltd and Equifax Inc and the lack of scrutiny by Equifax Ltd of Equifax Inc is the reason for this breach. 25.2 is violated for similar reasons, but also due to Equifax Ltd's inability to check whether all relevant UK personal data was deleted by Equifax Inc after processing.

Article 28 relates to the processors of the data, in this case, Equifax Inc. 28.1 states that 'the controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures'. The lack of due diligence by Equifax Ltd on Equifax Inc's systems and the substandard agreement between the Controller and Processor means that Equifax Ltd is in clear violation of 28.1. Equifax Ltd is also in violation of 28.3, points, c, e, f, g, h. These are violated for the same reasons as above, the lack of a contract between the controller and processor, that requires 'adequate safeguard / security requirements', the non-deletion/retuning of UK personal data by Equifax Inc to Equifax Ltd after processing, the lack of auditing by Equifax Ltd of Equifax Inc's systems, and breach of Articles 32 and 33, stated below.

Article 32 is regarding the security of processing. Equifax is in clear violation of the following with the reasons given above; 32.1.b, 32.1.c, 32.1.d, 32.2. It could also be argued that Equifax Inc could be in violation of 32.1.a due to the lack of encryption of user passwords.

Article 33 pertains to the notification of a personal data breach to the commissioner. Equifax Ltd is not in violation of this Article because once notified by Equifax Inc of the breach, it notified the ICO with delay. But Equifax Inc, the processor, only notified Equifax Ltd about one week after the discovery of the UK personal data breach (ICO V. Equifax Ltd, [2018]). This, in turn, puts Equifax Inc in violation of 33.2.

Under UK DPA 1998, The commissioner fined Equifax Ltd the maximum penalty of £500,000 (ICO V. Equifax Ltd, [2018]) for the severity of the breach. Under UK GDPR the highest fine is '£17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher' (ICO, 2021). Due to the severity of the breach, the author of this report believes that Equifax

Ltd would receive a substantial fine, possibly the maximum amount. This would be due to the substantial violations of the UK GDPR due to all the following reasons:

1. A lack of property auditing of Equifax Inc by Equifax Ltd
2. A lack of ‘adequate safeguards / security requirements’ in the contract between Equifax Ltd and Equifax Inc
3. A lack of safeguarding and scrutiny by Equifax Ltd to ensure the deletion/returning of UK personal data by Equifax Inc.
4. A lacking security assessment of Equifax Inc by Equifax Ltd
5. A lack of communication between Equifax Ltd and Equifax Inc resulted in at least one week delay in the reporting of the breach of UK personal data to the ICO.

Why do Data Breaches continue to happen?

The author of this report believes that data breaches continue to occur due to the lack of awareness of the importance of data privacy and the underestimation of cybersecurity events. Organizations are often optimistic and do not expect cyberattacks to happen. This blind optimism results in a lack of investment in cybersecurity, putting vital data at risk of a breach. As such, Organizations must take the necessary steps to ensure that their cybersecurity is sufficient and that employees have the necessary training to prevent cybersecurity incidents.

Section C

Introduction

AI adoption is increasing with IBM reporting an increase of 4% from 2021 to 2022. Organizations are harnessing data through the power of AI to revolutionize industries. This report will look into how new technologies, Data, and AI are pushing the boundaries of innovation to produce state-of-the-art capabilities. It will also include a case study of Spotify's use of AI to transform organizational decision-making.

The Role of New Technologies and Data in Finance

Citi Group states that 'Outside of Technology, the Banking and Securities sector is the biggest spender on external AI services and has fast growth' (Citi, 2018). The banking industry is at the forefront of adopting new technologies to build state-of-the-art capabilities.

The rise of FinTech is evident with Deloitte reporting the growth index of FinTech companies in the UK compared to SMEs being almost ten times greater in 2020 (Deloitte, 2020). FinTech companies make 'financial processes and traditional financial services more accessible using software' (Rutter, 2022), such as, by harnessing AI, Blockchain, and UX/UI development. For example, Monzo, through its easily accessible and convenient UI is considered a leading FinTech company with over 7 million UK customers (O'Brien, 2023).

BloombergGPT, released in March 2023, is the first Generative LLM, which has been 'specifically trained on a wide range of financial data' (Bloomberg, 2023). By harnessing the power of AI and NLP, Bloomberg has developed BloombergGPT which will assist in 'improving existing financial NLP tasks, such as sentiment analysis, named entity recognition, news classification, and question answering, among others' (Bloomberg, 2023).

The finance industry is being transformed by technology. This well-established industry is being forced to adopt new technologies as a central part of its infrastructure to meet the needs of the individual.

Case Study: Spotify

Spotify is one of the largest providers of digital music, podcast, and video services (Rutter, 2022) with over 515 million users (Rutter, 2022). AI is a central part of Spotify's business model, which hopes to attract users through user experience, specifically through recommendations. Spotify does this in 3 ways; Collaborative Filtering, NLP, and Audio Models (Oza, 2022).

Spotify uses collaborative filtering to track users' behavioral trends, which include most played songs, recently played songs, etc. Using AI, Spotify is able to analyze this data and apply a collaborative filter to generate song recommendations. It also uses this to generate each user's 'discover weekly playlists' (Oza, 2022). Spotify uses NLP models to track music industry trends across the internet. It then uses these trends to modify its recommendations. For example, Spotify may track the language used by an artist online and then recommend to listeners of that artist, songs based on that language (Oza, 2022). Spotify also uses an audio model for its recommendations. The audio model analyses the songs that the user listens to and recommends songs based on the similarities between them. This would be particularly useful for new artists who may not have lots of listeners and who do not have a large internet presence (Oza, 2022).

Spotify combines all of these methods to provide 'hyper-personalized recommendations' (Kaput, 2022) that keep it ahead of the competition.

Although Spotify already leverages the power of AI, it could take this further by experimenting with different AI models. For example, for music, they could use generative models to create AI-generated music. They could use AI to automatically summarise podcasts by generating a transcript to perform summarization on. This would considerably cut production time for developers, thus attracting more podcasts (Kaput, 2022).

Music streaming is not unique to Spotify, and consumers can access the same content through other streamers for a similar price. Spotify's business model strives on staying ahead of the competition with regard to its recommendation algorithm, which draws in more users with an annual increase of at least 14.9% since 2015 (Dean, 2021).

Data privacy, information governance

The UK has strict data privacy and information governance requirements under UK GDPR and DPA 2018. The ICO can heavily fine organizations that do not comply with the legislation. The author of the report believes that UK GPDR and DPA 2018 are robust and sufficient to protect the personal data of individuals. However the author believes that in cases of personal data breaches, organizations often play the victim when the real victims are the individuals whose personal data was breached. As such, the author believes that there needs to be firmer action by the ICO to ensure that organizations that have had a breach are properly punished, this is highly motivated by the fact British Airways had its fine for a severe breach of personal data reduced from £183 million to £20 million (BBC, 2020), which the author believes is unjust.

References

Arkin, R. (2010). *The case for ethical autonomy in unmanned systems*. [online] *Governing Lethal Behavior in Autonomous Robots*. Taylor & Francis Group. Available at: https://smartech.gatech.edu/bitstream/handle/1853/36516/Arkin_ethical_autonomous_systems_final.pdf?sequence=1&origin=publication_detail [Accessed 7 May 2023].

Austria (2023). *Working Paper submitted to the 2022 Chair of the Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS)* . [online] Available at: https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2023/gge/documents/Austria_March2023.pdf.

businesswire (2022). *Autonomous Military Weapons Global Market Report 2022: Significant Government Investment Driving Growth - ResearchAndMarkets.com*. [online] www.businesswire.com. Available at: https://www.businesswire.com/news/home/20220802005616/en/Autonomous-Military-Weapons-Global-Market-Report-2022-Significant-Government-Investment-Driving-Growth---ResearchAndMarkets.com#:~:text=The%20global%20autonomous%20military%20weapons [Accessed 9 May 2023].

Choudhury, L.M.R. (2021). *Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council*. [online] Available at: https://undocs.org/Home/Mobile?FinalSymbol=S%2F2021%2F229&Language=E&DeviceType=Desktop&LangRequested=False [Accessed 7 May 2023].

Etzioni, A. and Etzioni, A. (2018). Pros and Cons of Autonomous Weapons Systems (with Oren Etzioni). In: *Happiness is the Wrong Metric: A Liberal Communitarian Response to Populism*. [online] Cham: Springer International Publishing, pp.253–263. doi:https://doi.org/10.1007/9783319696232_16.

Gigova, R. (2017). *Who Putin thinks will rule the world*. [online] CNN. Available at: https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.

Heikkilä, M. (2022). *Why business is booming for military AI startups*. [online] MIT Technology Review. Available at: https://www.technologyreview.com/2022/07/07/1055526/why-business-is-booming-for-military-ai-startups/.

IHL (n.d.). *Rule 88. Non-Discrimination*. [online] Icrc.org. Available at: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule88.

Kayser, D. (2022). *Increasing autonomy in weapons systems: 10 examples that can inform thinking*. [online] Available at: https://www.stopkillerrobots.org/resource/increasing-autonomy-in-weapons-systems/ [Accessed 9 May 2023].

Reaching Critical Will (2023). *Documents*. [online] www.reachingcriticalwill.org. Available at: https://www.reachingcriticalwill.org/disarmament-fora/ccw/2023/laws/documents [Accessed 12 May 2023].

State of Palestine (2023). *State of Palestine's Proposal for the Normative and Operational Framework on Autonomous Weapons Systems*. [online] Available at: https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_WP.2_Rev.1.pdf [Accessed 7 May 2023].

Stop Killer Robots (2023). *States make progress on policy at UN discussions, as momentum builds towards Treaty on AWS*. [online] Stop Killer Robots. Available at: https://www.stopkillerrobots.org/news/states-make-progress-on-policy-at-un-discussions-as-momentum-builds-towards-treaty-on-aws/ [Accessed 8 May 2023].

StopKillerRobots (n.d.). *Emerging tech and artificial intelligence*. [online] Stop Killer Robots. Available at: https://www.stopkillerrobots.org/stop-killer-robots/emerging-tech-and-artificial-intelligence/ [Accessed 9 May 2023].

StopKillerRobots (n.d.). *Stop Killer Robots*. [online] Stop Killer Robots. Available at: https://www.stopkillerrobots.org/stop-killer-robots/facts-about-autonomous-weapons/ [Accessed 9 May 2023].

Surgeon General (2006). *Mental Health Advisory Team (MHAT) IV Operation Iraqi Freedom 05·07*. [online] Available at:

https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/PB2010103335.xhtml [Accessed 7 May 2023].

UNA (2023). *33 states call for urgent negotiation of new international law to limit autonomous weapons*. [online] UNA_UK. Available at: https://una.org.uk/news/33-states-call-for-urgent-negotiation-of-new-international-law-to-limit-autonomy-in-weapons-systems [Accessed 12 May 2023].

epic (2021). *EPIC - Equifax Data Breach*. [online] archive.epic.org. Available at: https://archive.epic.org/privacy/data-breach/equifax/.

Equifax (n.d.). *Company Profile - Equifax*. [online] Equifax. Available at: https://www.equifax.co.uk/about-equifax/company-profile/en_gb/.

Equifax (2023). *Who We Are*. [online] Equifax. Available at: https://www.equifax.com/about-equifax/who-we-are/.

Federal Trade Commission (2019). *Equifax to pay $575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach*. [online] Federal Trade Commission. Available at: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach.

IBM (2022). *Cost of a data breach 2022*. [online] Available at: https://www.ibm.com/reports/data-breach.

IBM (n.d.). *What is a Data Breach? | IBM*. [online] www.ibm.com. Available at: https://www.ibm.com/topics/data-breach#:~:text=A%20data%20breach%20is%20any%20security%20incident%20in%20which%20unauthorized.

ICO (2019). *Personal data breaches*. [online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/.

ICO (2021). *Penalties*. [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/penalties/.

ICO V. Equifax Ltd [2018] Available at: https://ico.org.uk/media/2259808/equifax-ltd-mpn-20180919.pdf.

UK GDPR. Available at: https://www.legislation.gov.uk/eur/2016/679/introduction.

BBC (2020). British Airways fined £20m over data breach. *BBC News*. [online] 16 Oct. Available at: https://www.bbc.co.uk/news/technology-54568784.

Bloomberg (2023). Introducing BloombergGPT, Bloomberg's 50-billion parameter large language model, purpose-built from scratch for finance | Press | Bloomberg LP. *Bloomberg L.P.* [online] 30 Mar. Available at: https://www.bloomberg.com/company/press/bloomberggpt-50-billion-parameter-llm-tuned-finance/.

Citi (2018). *The Bank of the Future*. [online] Available at: https://icg.citi.com/icghome/what-we-think/citigps/insights/bank-future.

Dean, B. (2021). *Spotify Usage and Growth Statistics: How Many People Use Spotify in 2021?* [online] Backlinko. Available at: https://backlinko.com/spotify-users.

Deloitte (2020). *The UK FinTech landscape*. [online] Deloitte United Kingdom. Available at: https://www2.deloitte.com/uk/en/pages/financial-services/articles/uk-fintech-landscape.html.

Kaput, M. (2022). *How Spotify Uses Artificial Intelligence—and What You Can Learn from It*. [online] www.marketingaiinstitute.com. Available at: https://www.marketingaiinstitute.com/blog/spotify-artificial-intelligence.

O'Brien, A. (2023). *Monzo revenues surge more than twofold, putting it on track for 2023 profitability | Sifted*. [online] Sifted. Available at: https://sifted.eu/articles/monzo-2022-revenue-surge-profitability.

Oza, H. (2022). *How Artificial Intelligence Helps Spotify Win In The Music Streaming World | HData Systems*. [online] www.hdatasystems.com. Available at: https://www.hdatasystems.com/blog/how-artificial-intelligence-helps-spotify-win-in-the-music-streaming-world.

Rutter, K. (2022). *What is fintech and why does it matter?* [online] www.lloydsbankinggroup.com. Available at: https://www.lloydsbankinggroup.com/insights/what-is-fintech-and-why-does-it-matter.html.

Spotify (2020). *What is Spotify?* [online] Spotify. Available at: https://support.spotify.com/us/article/what-is-spotify/.