The Modern Threat to Data Privacy

An analysis of the technological and legal response to an increase in threats to data privacy

Daniel Elston

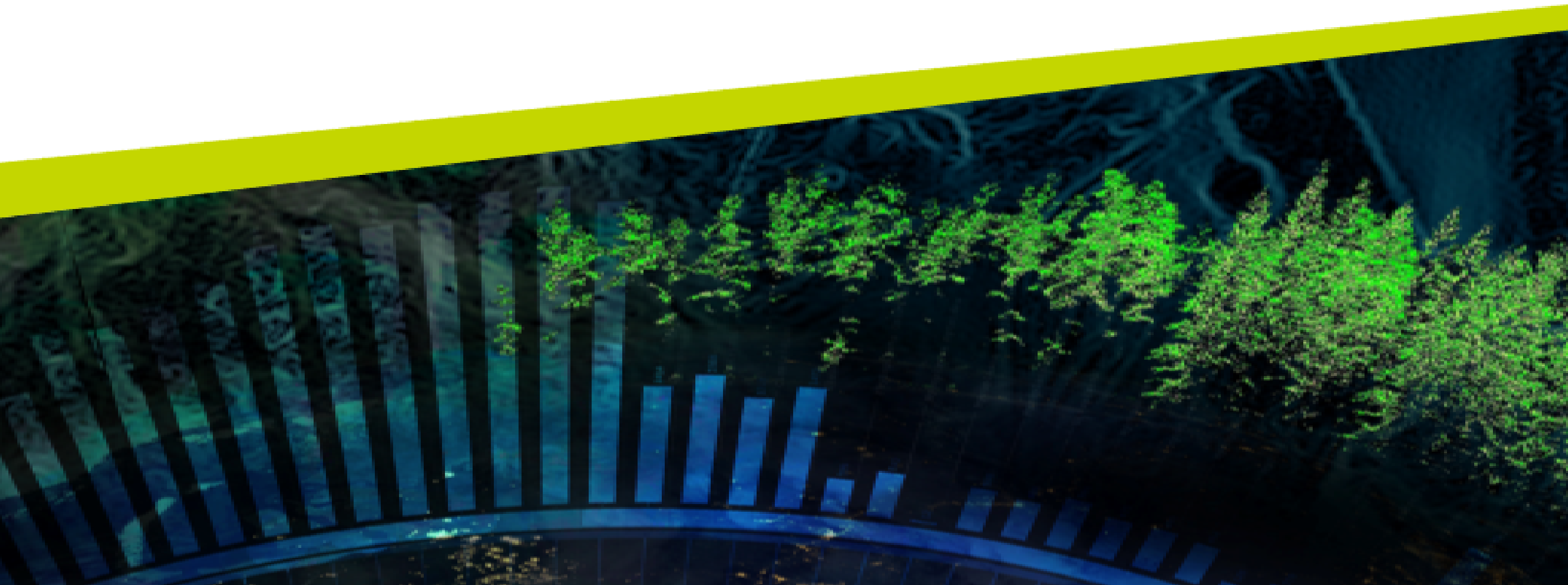
Email: ec21024@qmul.ac.uk
Student ID: 210720147

Submission Date: 03/05/2022
Word Count: 4928

Supervisor: Dr. Mahesha Samaratunga

MSc Data Science and Artificial Intelligence
Queen Mary University of London
School of Electronic Engineering and Computer Science

Ethics, Regulation and Law in Advanced Ditigal Information Processing and Decision Making
Module: ECS7025P



Executive Summary

This papers aims to identify and assess the legal and technological response to modern data privacy threats. statistics show that data breaches increase in both frequency and severity over time, with two thirds of all data breaches resulting from human error or hackers. This paper argues that increasing the cyber security practices employed by data controllers and processors would result in a decrease in data breaches. To accommodate an increase in cyber security, it is argued that a proactive approach must be employed. Technology must do more in terms of breach data collection while the law must impose further regulations and penalties, building on the principles. This paper also makes recommendations for improving data controllers risk analysis, organisational policies and technical measures.

Contents

Abbreviations

- **BA**: British Airways
- **CA**: Cambridge Analytica
- **CBI**: Cloud Business Intelligence
- **CMA**: Competition (and) Markets Authority
- **DPA**: Data Protection Act
- **DPD**: Data Protection Directive
- **DPO**: Data Protection Officer
- **EAD**: Ethically Aligned Design
- **GBP**: Great British Pound
- **GDPR**: General Data Protection Act
- **ICO**: Information Commissioners Office
- **IT**: Information Technology
- **MI**: Marriott International
- **QMUL**: Queen Mary University (of) London

Introduction

The modern threat to data privacy does not only come in the form of data breaches. A large contribution to this threat is the law itself, or lack thereof. The GPDR [1] is a substantial development from the previous DPA [2]. However, the GDPR still fails to hold companies appropriately accountable for their violations of its regulations. The GDPR further fails in practical application, resulting in complications in consent and longevity. For the purpose of this essay, issues regarding private data and its protection are explored due to an ever-increasing technological advancement threatening to make the GDPR and current protection techniques redundant, unless appropriate action is taken.

To make this argument, this paper will firstly highlight the modern threats to private data, including how it can be used against the data subject and that utilising technology alone is, at present, not the solution. This essay goes on to discuss the MI data breach of 2018. This breach resulted in a loss of data subjects' private data and revealed the senior management's flagrant violations of ethics and GDPR principles.

This paper will then outline the measures that should be taken to prevent data breaches. Specifically, a proactive approach to preparing staff and systems for a potential threat will be recommended alongside an increase to the already severe penalties for violating the GDPR and therefore, human rights.

In terms of law and regulation, this paper will highlight the serious failings of the GDPR and suggest improvements that would result in data controllers and processors improving all aspects of their cyber security.

Finally, this paper hypothesises a 'perfect' legal response that suggests how the GDPR could be appropriately adapted to accommodate an ever-changing technological advancement.

Section A - Literature Review

Big data is of great interest in research, business, economic and social studies [3]. This is due to big data having large scale potential societal benefits. An example can be seen in the healthcare sector, where big data can be used to inform healthcare professional decision making [4]. All forms of data have varying degrees of benefit for society but access to private data, such as medical data, is becoming more restricted. This is due to private data being misused in malicious ways, prompting the data subject to withdraw from data gathering practices.

This literature review aims to summarise current research regarding threats to private data and its preservation, while suggesting further areas of research. To address the problem with data privacy, laws regarding the rapid advancement of technology will be discussed. The importance of data privacy is demonstrated by the potential societal impact of big data; for instance, the sooner privacy is guaranteed, the sooner unlimited data can be collected and utilised.

Defining Data Privacy

The right to privacy is recognised as a 'universal human right', as stated in article 8 of the European Convention of Human Rights (2012). A modern adaptation of this results in the right to data protection [5]. Personal data is defined as any information relating to the identification of a data subject. Examples of such data includes bio-metric data, IP addresses and dates of birth. It is now accepted that data privacy is a universal human right.

Privacy is not only an individual right but also a social value. Solove defines privacy as "an umbrella term, referring to a wide and disparate group of related things" [6]. Splitting data privacy into 2 categories, communication and information, private data can be defined as information shared between two parties that is carried between any medium and personal data that is collected and processed by an organisation [7]. It can then be argued that having any form of interaction with this data without the data subject's consent is a violation of data privacy.

A Previous Violation of Data Privacy

The case of CA highlighted both the vulnerability and the potential for misuse of private data. Facebook handed over personal data of more than 87 million subjects to CA [8], a data controller that used private data to profile each subject for political gain. This case highlights the amount of sensitive private data generated by modern technology today and its potential for misuse.

This heavily publicised breach forced law makers into action. Regulations were created that valued data privacy while attempting to hold data controllers and processors accountable. The CA case instilled a distrust of big data controllers, who were perceived as highly irresponsible and cunning,exercising little regard for the ethical implications of their use of private data.

Misuse of Private Data

Identification connects an identifier such as a person's name or address with an individual entity [9]. Personal medical data for example, is vital in research and so is stored confidentiality via data anonymisation. However, there is still a $0.09 - 0.05$ probability that identification can occur [10]. Digital profiling is the practise of using a data subject's private data to profile and evaluate personal attributes [11]. This can be used to predict a person's economical situation, habits, interests and behaviours which can then be used unfavourably against the subject, whether it be capitalising on a person's spending trends or targeting specific adds to them with malicious intent. Digital profiling can be automatic, seen by the use of cookies, which allowed the unobtrusive collection of personal data not limited by ethics [12].

Businesses can benefit from big data by using it to inform decision-making. CBI is the practice of storing and utilising big data, supporting an increase in efficiency and profitability of a business. The amount of data stored on the cloud may exceed the Petabyte (1015) scale [13]. Cloud computing has many advantages, such as a seemingly endless amount of storage. However, there are also disadvantages; most significantly, even a single attacker could lead to severe data breaches resulting in private data being lost via identification, DoS attacks or eavesdropping [14].

Private Data Preservation Techniques

Anonymisation techniques employ algorithms to 'scramble' personal data, so if a breach was to occur, it would be more difficult to identify a person. This would further reduce digital profiling. There exist many anonymisation methods to improve security of private data [15]. However each method is weak in a particular area and there exists a trade off between complexity, security and resultant data quality [16]. Further research into such models may be futile as it is unlikely that 100% anonymisation will occur from a model alone. However, it is stated that only 15 demographic attributes are required to make a person 0.9998 unique [17]. It is therefore suggested that obtaining more demographic attributes should be the focus of improving anonymisation.

A recent paper has suggested interviewing system architects and users to get their input on the weaknesses of the Cloud [14]. This will result in raw data which can be utilised by future architects as well as security maintenance specialists. A regular supply of such data will allow for a more proactive approach to defending against potential threats.

As with all forms of human rights violations, the law will likely have the largest effect in reducing both the rate and severity of data breaches. By holding those in positions of responsibility accountable, an all-encompassing improvement of cyber security can be observed. Furthermore, the law attempts to ensure that ethical violations are avoided through the use of regulations and strict policies. For instance, Principle 2 of the GDPR and Article 22 regulate automated individual decision-making, including profiling.

Comments on Current Private Data Landscape

Current research regarding data privacy and its preservation must be improved. An increase in privacy preservation techniques is needed to mirror the increase in data breach frequency and severity seen in 1. It would be simple to assume that the increase seen in 1 is due to a lack of current knowledge surrounding data security, but it can be argued that many mid-large scale data controllers, that are often the focus of data breaches, are not doing enough. This is demonstrated by the MI case, where the controller appeared to prioritise profit-making above data security. The systems in use resembled legacy rather than advanced. By implementing regulations that hold data controllers accountable for the security of private data, improvements can be made. The GDPR is a good start but it is far from the perfect response.

Nevertheless, even with state-of-the-art technology and rigorous regulations in place, flaws in security would likely continue to exist in the healthcare sector [16]. To summarise further areas of research for data privacy preservation techniques, pro-activity is needed. Whether it be in the form of data collection, policy creation or more advanced algorithms. A proactive approach to anticipating and mitigating breaches could see a blunt to the large spikes that are seen in 1 in recent years. The sentiment remains that data breaches are for now, a regular occurrence. While this is the case, the only rejoice seems to be the fact that the constant struggle for privacy is accelerating knowledge and research to an inevitable excellence.

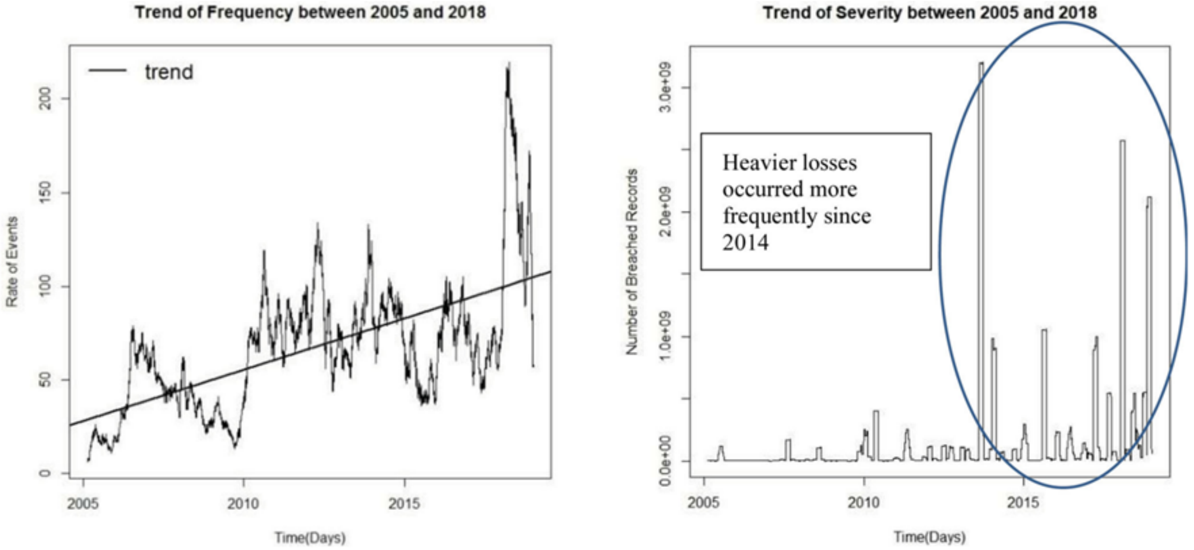
Section B - Research and Discussion

Despite advancements in research and regulations, private data is less secure than ever. To address this, the GDPR has set out to impose strict regulations in regard to data privacy and ethics while also providing a legal spotlight on the matter. Data anonymisation and storage systems continue to improve however data breaches persist, highlighted by the MI case of 2018.

Data Breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes [18].

Data breaches occur mostly for either financial gain or espionage purposes. As for how breaches occur, recent studies suggest that data breaches are caused by human error (33.5%), misuse of data (29.5%), theft (16.3%), hacking (14.8%) and malware (10.8%) [19]. Over 80% of the data breaches occurring between 2005-2018 were caused by hackers or malware, physical loss, lost or stolen portable devices and unintended disclosure of information (human error). The most devastating breaches target big companies such as Yahoo, Facebook or MI [20].


Trend of Frequency between 2005 and 2018

Trend of Severity between 2005 and 2018

Heavier losses occurred more frequently since 2014

Figure 1: Trends in Frequency and Severity of Data Breach Risk Between 2005 and 2018 [21].

The Marriott International Case (2018)

MI is an American hotel chain of greater than 6500 hotels over 127 countries. It is the largest hotel chain in the world who were also the first to implement the online reservation of hotels, giving potential insight into how long private data has been gathered and potentially stored. MI generated approximately 8.10 billion GBP in 2020 and approximately 10.49 billion GBP in 2021.

An unknown cyber-attacker installed malware into Starwood's system in 2014. This gave the attacker remote access to the network where they would then go on to reproduce the private data of data subjects. MI would go on to acquire Starwood in 2016, however it is not until 2018 that the malware was detected by MI's IT contractor Accenture. By this time, it was approximated that the personal data of 383 million data subjects was compromised. A further estimated 500 million records were breached in 2020. The nature of the data breached included passport numbers, names, dates of birth, credit card information and home addresses along with hundreds of millions of location histories of individuals [22]. A visual of the full timeline can be seen in figure 2.

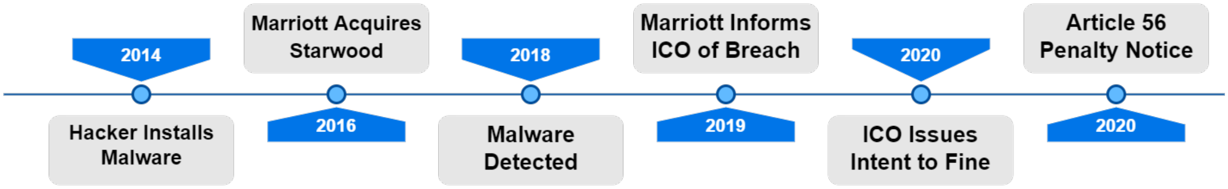

2014
Hacker Installs Malware
Marriott Acquires Starwood
2016
2018
Malware Detected
Marriott Informs ICO of Breach
2019
2020
ICO Issues Intent to Fine
Article 56 Penalty Notice
2020

Figure 2: Timeline of MI case from initial breach to issue of penalty notice by ICO.

MI relied heavily on the use of big data to drive business growth and profits through the use of data driven marketing campaigns and loyalty programmes. The sensitive nature of the details collected by MI should have prompted senior management to review their cyber security when handling such private data. Couple this with the fact both MI and Starwood were subject to many breaches involving malware in the years prior to the 2018 mega-breach [22], and in general data breaches were on the rise in both number and severity, an internal review of cyber security standards should have been paramount years prior.

Human error and misuse of data can make up nearly two thirds of data breaches. Incorporate these figures with the assumption that MI was using a system highly vulnerable to cyber attack, and the fact that it nearly disregarded proactive cyber security practices, a large data breach seems certain. The question remains, why was cyber security not increased drastically, or at very least reviewed.

UK DPA, GDPR & ICO

The DPA 2018 sets out the framework for data protection law in the UK. The GDPR supplements the DPA providing a wider scope. The GDPR is a form of data protection law, introduced as a much-needed improvement on the DPD, implemented to address rapid technological developments [23] and give back control of private data to the data subject. The GDPR is a set of regulations a company must follow in order to lawfully obtain and process personal data. The 7 principles of data privacy set out in the GDPR are:

- **Lawfulness, fairness and transparency**: Companies must have legal basis for processing a person's data. Companies must be upfront, fair, transparent, clear and honest of how and why a company is collecting data as well as how they intend to process it;

- **Purpose limitation**: Data collected is for a specific, explicit and legitimate reason. Data use must be specified and cannot be used for any other reason;

- **Data Minimisation**: Only collect the minimum amount of personal data required for specified task;

- **Accuracy**: Data collected is accurate and complete. Incomplete data must be corrected or deleted where appropriate;

- **Storage limitation**: Justifications must be made for time a company is storing personal data. Data subjects must be informed of companies intended storage time period. Company is required to delete data in a timely manner and cannot store data for an unreasonable amount of time;

- **Integrity and Confidentiality**: Companies must maintain a degree of confidentiality regarding personal data collected. Certain levels of security including encryption, must be upheld when handling personal data; and

- **Accountability**: Companies must demonstrate and keep audited records of how they comply with GDPR, following the correct protocols throughout.

The ICO is tasked with holding companies accountable when they do not follow the GDPR. The ICO follows a process of notifying, investigating, issuing an intent to fine and applying monetary penalties to companies who do not comply with or violate the GDPR. The ICO further checks if there is a serious enough violation of the GDPR to warrant a penalty. The ICO tasks include:

- **Enforcement action**: Issuing penalty notices and potentially fining companies that do not comply with or violate the GDPR;
- **Decision notes**: Making decisions if company has complied with the GDPR, while making recommendations for compliance measures;
- **Audits and overview**: Assessing whether effective security controls have been put in place by a company, supporting the obligation of a company to protect personal data; and
- **Monitoring compliance**: Ensuring that when a company detects a breach, it is reported within 72 hours.

Marriott International GDPR & Ethical Violations

Lead supervisory authority the ICO, fined MI under section 2 of the GDPR, Security of personal data and section 3 of the DPA, Law enforcement processing. The security principle requires a data controller to process personal data securely by means of 'appropriate technical and organisational measures'. Practices such as risk analysis, organisational policies, and physical and technical measures must be conducted. Additional requirements must also be considered regarding the security of processing practices. MI grossly violated the security principles by disregarding the set standards of personal data security in many ways. The ICO found the following points were in breach of the GDPR and therefore sufficient reason to fine:

- Insufficient monitoring of privileged accounts that would have detected the breach;
- Insufficient monitoring of databases;
- Failure to implement measures to reduce vulnerability of the server; and
- Failure to encrypt certain personal data.

Further notable failures included a lack of understanding or disregard for current levels of cyber threats, failure to correctly evaluate security needs and lack of due diligence when acquiring Starwood.

To understand the underlying ethical violations, the UK Data Ethic framework must be reviewed. Principles 2, 3 and 5 had been disregarded by MI. MI did not sufficiently diversify their expertise, as demonstrated by the lack of cyber security staff either present at the company or speaking out to the violations, thereby infringing principle 2. MI did not confer with a DPO when conducting DPIA, violating principle 3.1. If they had satisfied this requirement, more rigorous security would likely have been in place. MI's accountability was further in question, hinting at a possible infringement of principle 3.4. The most flagrant violation of section 3 is subsection 3.3, Data Protection by Design. This is a legal requirement under the GDPR.

Consequences of Violations

As a result of such violations, MI was issued with the second largest data breach fine (18.4 million GBP), next to BA in 2020 (20 million GBP). A standard fine from ICO is around 4% of a company's annual turnover which is no small fee. The initial penalty notice was reduced due to mitigating factors.

As MI did not benefit financially from the breach, showed negligence but not intent, extended full cooperation to the ICO with respect to the investigation and it was their first offence, the fine was reduced. MI had attempted to reduce the fine further by blaming their IT contractor, but this was rejected by the ICO as MI was the controller.

Section C - Recommendations

This report makes its argument through the authors own individual research and summary points obtained from the QMUL Q-legal department. Further to this research, an interview has been conducted with a trainee solicitor well-versed in matters of data privacy and the GDPR, referred to as Respondent throughout.

Learning from the Marriott International Case

The first lesson to be learnt from the MI case is the need for data controllers and processors to conduct the correct risk analysis and have appropriate awareness of the technological climate. An increase in overall cyber security encapsulates this point and has been further proven by the ICO's finding on MI's breaches of the GDPR; with improved monitoring of privileged accounts and databases, the breach could have been detected sooner. Furthermore, had data been encrypted and legacy systems updated, private data would not be left so vulnerable. Even a superficial risk analysis could have had a similar effect. This shows the importance of senior management possessing an understanding and awareness of the risks and their cyber security systems and practices.

A further lesson to be learnt from the MI case is the necessity for a company to conduct the proper due diligence when acquiring companies. When questioned on the importance of due diligence, the Respondent (2022) stated that "failing to perform the correct due diligence not only puts the company at legal, financial and reputational risk but it also has an impact on data subjects. It is the acquiring company's responsibility to make sure data and privacy, or collection methods are sound, including any relationships with contractors". Regarding what advice the Respondent (2022) would extend to an acquiring company, it is recommended that they "obtain warranties from a company stating that these issues do not exist to further improve your due diligence process and provide legal protection in the instance of a data breach".

Preventing Data Breaches

Human error is a lead cause of data breaches; therefore, it is firstly suggested that regular training requirements be strictly imposed on all data controllers and processors. This would ensure that controllers and processors maintain the latest knowledge on data privacy. A second arm of this training would enforce an organisational security culture to a level at which employees are trained to identify symptoms of a potential insider threat. This should be supplemented with internal policies on how to handle such a threat and when to report such threats [24]. To supplement this, specific and thorough training on whistle-blowing policies should be provided to all relevant staff. This will ensure lower level controllers and processors can recognise areas of high breach risk, further reducing breach frequency and severity.

This training should facilitate the development of a heightened awareness of both the importance of private data security and threat, potentially reducing the frequency of breaches. Training could spark an increase in overall awareness of the threat to private data throughout all levels of a company, broadening the focus beyond the expertise of upper management that was observed in the analysis of the MI case. An increase in awareness at all levels is desirable as it could prompt senior management to implement action that would increase cyber security in compliance with the GDPR.

Problems with the GDPR

The GDPR is a good first step in getting data controllers and processors up to date in terms of cyber and data security while also holding them accountable for their actions. The GDPR provides an acceptable foundational level of protection in terms of ethics and human rights by having a wide scope. However, considering data privacy is a human right, the GDPR does not do enough to prevent breach.

The violation of universal human rights should and have appropriate consequences. This is the first failing of the GDPR: data breaches are not followed by sufficiently harsh consequences. "The ICO can issue fines up to 4% of global turnover or 20 million GBP. By comparison, the CMA can fine up to 10% of a company's global turnover for matters that do not concern human rights", Respondent (2022) outlines. The sanctions available to the CMA demonstrates that not only is a greater deterrent for violating the GDPR needed, but it is also an achievable concept.

The GDPR aims to place data subjects in a level of greater control regarding their personal data. Similarly, to the issue of consent, this can only be utilised should the data subject have a knowledge of their rights. A general lack of public awareness is proven by an online survey where 26% of individuals had a vague understanding of the GDPR and 21% had never heard of it [25]. If data subjects do not exercise their rights, due to lack of understanding or otherwise, privacy cannot be ensured.

Additionally, the GDPR fails to account for issues such as digital profiling, highlighted by the issue of consent. Consent is a ground for personal data processing, outlined in principle 7 of the GDPR, which may seem ideal in theory but is inherently problematic. In practicality, consent obtained in the digital consumer landscape is not freely given, specific, informed and unambiguous [26]. Respondent (2022) adds that "this is in part due to privacy policies being inaccessible by much of the population. This is, in part, due to the use of the complex technical language involved in data processing. As a result, informed consent is rarely provided. However, simplifying privacy policies to be understood by every individual similarly risks losing informed consent as the required detail is not provided". This trade-off further portrays how the GDPR is flawed and is not an adequate response to the current challenges.

Alongside the issue that private data is not sufficiently safe from potential breaches, it is argued that the GDPR fails the data subject in many ways. Instead of protecting private data, the GDPR is a list of guidelines that mitigate the frequency and severity of data breaches for companies. Furthermore, it places only a superficial level of control in the hands of the data subject.

Improving the GDPR

It is argued that harsher penalties should be placed on companies that violate the GDPR. The greater sanctions available to the CMA demonstrate that this is a realistic reform; a data controller or processor should be handed greater penalties in response to the violation of human rights in the context of private data. A further suggestion is that building on the current penalty system, a tiered penalty system should be applied to larger companies. A company with a greater amount of private data to keep secure would therefore have a greater threat of breach with far greater potential breach severity. Penalties should therefore be in line with potential breach severity and frequency, mirroring the data controller's and processor's responsibility.

Had the GDPR applied consumer protection laws, Respondent (2022) outlines that "the scope of protection would have increased in areas of inadequacy. For example, consumer law could be used to analyse the fairness of the conditions under which consumers agree to the processing of personal data, thereby providing additional protection in relation to privacy policies". A hypothesised 'fairness test' could be used to limit the abuse of consent as a legitimate ground for data processing, thereby addressing the criticisms discussed above [27]. Furthermore, an easy to implement short term correction could be to simply summarise privacy policies, potentially with a uniform layout. Admittedly, there is a risk that insufficient information will be provided (as discussed above). However, on the basis that users can begin to understand the ways in which they provide consent and what for, this compromise should be viewed as acceptable.

Whilst data privacy is based upon individual fairness and fundamental rights, consumer protection law is concerned with fairness in the broader commercial relationships [27]. Personal data has become an economic value, had the GDPR employed consumer protection law, a wider scope of analysis could have been introduced to data subject rights in the commercial context. For this reason, the GDPR could be reformed to incorporate consumer protection law.

Further considerations must be made in relation to the GDPR's polices, penalties and overall scope, in order to better serve the data subject. There exists a disconnect between the GDPR and the data subject, where theory and its practical application seem distant. It is therefore concluded that the GDPR is unable to properly deal with the issues posed by data privacy, big data and technology. To use the full potential of the GDPR, it must evolve along with the rapid advancement of the digital age in order to stay up to date and relevant in terms of modern threats to data.

A "Perfect" Legal Response

While it is important to improve the GDPR in the context of the technological climate that is comprehensible today, adapting the regulations to prepare for the future advancement of technology would see it remain a useful resource for years to come. The question now becomes: how to adapt the GDPR to the ever-changing technological climate? To 'future proof' the GDPR, a compromise must be met between detailed and vague regulations. As an example, an extremely vague law could encapsulate many areas of human rights, whereas an extremely detailed law can only encapsulate a particular instance. The problems lay where a balance must be met between vague and detailed, which does not fully address either problem. Highly detailed GDPR regulation is unable to address future potential threats. By contrast, a very vague regulation is better at accounting for future threats but risks providing inadequate solutions to current threats.

Constantly updating regulations in line with new emerging data privacy threats is a potential solution to the problem but opposes the proactive approach argued in this report, the former relies on waiting a breach to occur before addressing it. However, proactively anticipating threats and creating regulations to address them risks restricting technological advancement.

The perfect legal response to this problem would be to closely monitor technology and its advancement. Further monitoring of potential threats to human rights or the EAD [28] is also required. Once a threat is identified, proactively addressing it through constant GDPR regulation updates could provide a solution to the issue.

Conclusion

Private data breaches are increasing in both frequency and severity. To address these issues, a drastic increase in the average level of cyber security employed by both data controllers and processors is required. To facilitate this, it is suggested that a proactive approach is taken regarding cyber security and law implementation.

To improve cyber security, it is argued that a mandatory training programme for data controllers and processors together with an increase in overall awareness of threats to private data should yield the required results by reducing human error. Furthermore, collecting data regarding weakness in security systems could see a reduction in hacker incidents while further collecting a greater number of private data attributes would yield greater anonymisation results. These strategies would contribute to the reduction of frequency and severity of data breaches.

An analysis of the GDPR and MI data breach highlights the current problems in data privacy law. It has been argued that the GDPR is not a sufficient legal response to the current problems posed by the increasing technological advancement. While it does improve cyber security standards and tries returning control of private data back to the data subject, the GDPR ultimately fails to yield acceptable results. With accountability and lack of real-world application being the main problems, increasing GDPR violation penalties and implementing a breach severity tiered penalty system would result in data controllers and processors being held accountable to a greater degree. This could prompt senior management to improve cyber security while further improving awareness. It is also argued that should the GDPR apply consumer protection laws; a far greater scope of protection could be utilised regarding the data subject.

Finally, a ’perfect legal response’ is hypothesised to address the ever-emerging threats resulting from the increase in technological advancement which risks leaving the GDPR outdated. It is argued that closely monitoring technology as it advances and proactively addressing threats to human rights and the EAD would see data controllers and processors stay updated in their cyber security, reducing private data breaches.

References

[1] GDPR. Guide to the general data protection regulation, 2018.

[2] Data Protection Act. Data protection act 2018, 2018.

[3] Celina Rebello and Elaine Tavares. Big data privacy context: Literature effects on secure informational assets. *arXiv preprint arXiv:1808.08537*, 2018.

[4] Roberta Pastorino, Corrado De Vito, Giuseppe Migliara, Katrin Glocker, Ilona Binenbaum, Walter Ricciardi, and Stefania Boccia. Benefits and challenges of big data in healthcare: an overview of the european initiatives. *European journal of public health*, 29(Supplement_3):23–27, 2019.

[5] R Alonso García. The general provisions of the charter of fundamental rights of the european union. *European Law Journal*, 8(4):492–514, 2002.

[6] Daniel J Solove. A taxonomy of privacy. *U. Pa. l. Rev.*, 154:477, 2005.

[7] Lorna Stefanick. *Controlling knowledge: Freedom of information and privacy protection in a networked world*. Athabasca University Press, 2011.

[8] Jim Isaak and Mina J Hanna. User data privacy: Facebook, cambridge analytica, and privacy protection. *Computer*, 51(8):56–59, 2018.

[9] Noura Aleisa and Karen Renaud. Privacy of the internet of things: a systematic literature review (extended discussion). *arXiv preprint arXiv:1611.03340*, 2016.

[10] Anna Antoniou, Giacomo Dossena, Julia MacMillan, Steven Hamblin, David Clifton, and Paula Petrone. Assessing the risk of re-identification arising from an attack on anonymised data. *arXiv preprint arXiv:2203.16921*, 2022.

[11] S Murali Krishna, AP Siva Kumar, et al. Modern privacy threats and privacy preservation techniques in data analytics. In *Factoring Ethics in Technology, Policy Making and Regulation*. IntechOpen, 2021.

[12] Jo Pierson and Rob Heyman. Social media and cookies: challenges for online privacy. *info*, 2011.

[13] Hussain Al-Aqrabi, Lu Liu, Richard Hill, and Nick Antonopoulos. Cloud bi: Future of business intelligence in the cloud. *Journal of Computer and System Sciences*, 81(1):85–96, 2015.

[14] Jiyuan Zhang. A systematic literature review of data privacy issues in cloud bi. 2021.

[15] Yavuz Canbay, Seref Sagiroglu, and Yilmaz Vural. A new utility-aware anonymization model for privacy preserving data publishing. *Concurrency and Computation: Practice and Experience*, page e6808, 2022.

[16] Iyiola E Olatunji, Jens Rauch, Matthias Katzensteiner, and Megha Khosla. A review of anonymization for healthcare data. *Big Data*, 2022.

[17] Weiyi Xia, Yongtai Liu, Zhiyu Wan, Yevgeniy Vorobeychik, Murat Kantacioglu, Steve Nyemba, Ellen Wright Clayton, and Bradley A Malin. Enabling realistic health data re-identification risk assessment through adversarial modeling. *Journal of the American Medical Informatics Association*, 28(4):744–752, 2021.

[18] Alexandros Varveris and Fereniki Panagopoulou. The challenge of personal data protection in the digital era and global responses. In *Human Rights, Digital Society and the Law*, pages 273–285. Routledge, 2019.

[19] Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. Healthcare data breaches: insights and implications. In *Healthcare*, volume 8, page 133. Multidisciplinary Digital Publishing Institute, 2020.

[20] Hicham Hammouchi, Othmane Cherqi, Ghita Mezzour, Mounir Ghogho, and Mohammed El Koutbi. Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, 151:1004–1009, 2019.

[21] Kwangmin Jung. Extreme data breach losses: An alternative approach to estimating probable maximum loss for data breach risk. *North American Actuarial Journal*, 25(4):580–603, 2021.

[22] Neil Daswani and Moudy Elbayadi. The marriott breach. In *Big Breaches*, pages 55–74. Springer, 2021.

[23] Michael D Birnhack. The eu data protection directive: An engine of a global regime. *Computer Law & Security Review*, 24(6):508–520, 2008.

[24] Michael Samuel Ofori-Duodu. *Exploring Data Security Management Strategies for Preventing Data Breaches*. PhD thesis, Walden University, 2019.

[25] Daniela Messina. Online platforms, profiling, and artificial intelligence: new challenges for the gdpr and, in particular, for the informed and unambiguous data subject's consent, 2019.

[26] Wanda Presthus and Hanne Sørum. Are consumers concerned about privacy? an online survey emphasizing the general data protection regulation. *Procedia Computer Science*, 138:603–611, 2018.

[27] Natali Helberger and Agustin Reyna. The perfect match? a closer look at the relationship between eu consumer law and data protection law. *Common Market Law Review*, 54(5), 2017.

[28] Raja Chatila and John C Havens. The ieee global initiative on ethics of autonomous and intelligent systems, 2019.