The Marriott Data Breach: Data Protection and Privacy Safeguards Considerations

Name: Kweku Esuon Acquaye

ETHICS IN ADVANCED DIGITAL INFORMATION PROCESSING

Word Count: 4,946

Data Science and Artificial Intelligence

Table of Contents

List of Abbreviations and Glossary

AI	-	artificial intelligence
BA	-	British Airways
DPA	-	Data Protection Act
DPO	-	Data Protection Officer
EAD	-	ethically aligned design
EU	-	European Union
GDPR	-	General Data Protection Regulation
GP	-	General Practitioner
GPDPR	-	General Practice Data for Planning and Research
ICO	-	Information Commissioner's Office
IEEE	-	Institute of Electrical and Electronics Engineers
IP	-	internet protocol
ISO	-	International Organisation for Standards
IT	-	information technology
MFA	-	multi-factor authentication
NHS	-	National Health Service
PII	-	personal identifiable information
TATI	-	The Alan Turing Institute
UK	-	United Kingdom
USA	-	United States of America
USB	-	universal serial bus

List of Figures

Executive Summary

The digital age is here, and the adoption of a digital future for humankind can no longer be deferred. Every passing year sees more of our lives being moved online or digitised in one way or another, from the mundane to the most serious. The danger of losing complete privacy and hence our individuality rises in direct proportion with our increasingly digitised lives. As humans however, there are vestiges of our individual identities we cherish that ought to remain private, from medical conditions and individual genomes to bank card details. That is why the issue of Data Protection and Privacy Safeguards has become one of the most pertinent issues of our time. Its importance cannot be overemphasised.

The Marriott Data Breach of 2014 to 2018 constitutes one of the most serious and appalling data protection failures of modern times. Data comprising the personal details of up to 500 million customers (conservative estimate, (Fruhlinger, 2020)) was compromised for the better part of 4 years before discovery of the systems intrusion, following Starwood Hotels' acquisition by Marriott in 2016. Compromised data included full names, email addresses, locations with dates and times, and passport numbers (Afifi-Sabet, 2020). On 30th October 2020 the United Kingdom (UK) Information Commissioner's Office (ICO) issued a fine of £18.4 million, from an initially proposed £99.2 million.

As if the data breach itself was not bad enough, a cottage industry developed in its wake where other malfeasants successfully compromised others by sending phishing emails ostensibly from Marriott Inc with links asking people to reset their passwords.

In this report, an extensive review of the literature on the issue of data protection and privacy safeguards is attempted. This is then related to the Marriott case in regard of GDPR and DPA in order to understand it. Secondary data gathering of published resources is then carried out, drawing in insights from the Lesson 4 Lecture. Further insights are drawn from an interview with the DPO of a Tech Startup (Appendix 3), and a critical appraisal of all the information undertaken. The personal considerations and opinions of this author feature heavily in this report.

Conclusions such as the need to empower technical law officers to proactively audit the infrastructure and IT systems of organisations are drawn. Lessons learned such as the need for persistent systems monitoring and high level of security training and awareness for all employees are enumerated, and policy recommendations to the ICO such as making data encryption mandatory by law are suggested.

Section A

Literature Review

Current definitions and how do they differ/overlap in terms of the literature
Data Protection is essentially the safekeeping of personal identifiable information (PII) from being disseminated to unauthorised persons, and especially from falling into the wrong hands, i.e. those who would use it for malicious purposes. PII consists of details such as full name, date of birth, full address, national insurance (NI in UK) or social security (SS in USA) number, passport number, or any other information that can be used – by itself or in conjunction with other information – to identify an individual human person.

Over the years the definition of "data protection" and associated terms have evolved.

The UK Data Protection Act (DPA) 1998 defined personal data as " … *data relating to a living individual who can be identified from that data; or from that data plus other information that was in the possession, or likely to come into the possession, of the data controller* … ". This definition made a distinction between *personal data* and *sensitive personal data*, the latter which " … *concerned the subject's race, ethnicity, politics, religion, trade union status, health, sexual history, or criminal record ...* " (Appendix 2).

The ICO currently defines personal data as " … *information that relates to an identified or identifiable individual* … ", and " … *could include other identifiers such as an IP address or a cookie identifier* … " (ICO 2021). This definition in the DPA 2018 updates personal data to include online and digital data such as IP addresses and cookie identifiers.

The European Union (EU), under its General Data Protection Regulation (GDPR), defines personal data as " … *any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological,* ***genetic****, mental, economic, cultural or social identity of that person* … ".

It is observed from the literature that the definition of personal data has evolved over the years to include additional identifiers such as location data, genetic and biometric data, as well as economic, cultural, and social identities. The UK was a signatory and participant of the EU GDPR 2016 until 25th May 2018 when it was replaced by the UK DPA 2018. The latter act was then further replaced on 1st January 2021 by the EU (Withdrawal) Act 2018 updating the UK's status outside the EU. It is noted that this definition continues to automatically include what the UK separately defines as *sensitive data*.

How the literature around data protection has evolved

Privacy Safeguards concern the guidelines, recommendations, legislation, actions, and practices that mitigate the risk of contravening data protection and thereby resulting in the loss of personal data. It proposes, promotes, and promulgates actions such as measures to secure software and hardware, appropriate security awareness and training for employees, and the implementation of technical solutions to forestall personal data loss.

The Harvard Law Review article "Right to Privacy" (Warren and Brandeis, 1890), is one of the earliest known works on the subject of privacy. It influenced and developed the notion of *privacy protected by law*, later adopted not only in the USA but also in Europe, UK and across the world. Its context and similarity to the current privacy debate is that it was written at a time of technological change, i.e. photography in journalism at a time when newspapers could publish disparaging photographs of individuals without their consent or notification. Brandeis and Warren promoted the argument, novel at the time, that " … *the right to be let alone ought to be secured against invasion except for some compelling reason of public welfare* ... ", and that this was indispensable to personal integrity and ought to be protected by law (Warren and Brandeis, 1890). Their argument gained widespread support but was also resisted by a minority who perceived their monetary interests threatened.

It is apparent from the literature that most publications subscribe to the Alan Westin definition of privacy, which is " … *the prerogative and claim of individuals, groups and institutions to determine for themselves when, how, and what extent information about them is communicated to others* … ", and also " … *the right of the individual to control, edit, manage, and delete information about themselves* … " (Westin, 1967). It is the view of this report author that not only was this definition adequate for the period from the 1960s (when Professor Westin's seminal work was published) up to the mid 1980s (the dawn of the digital age), but also visionary for the current raging debates on this issue. The Westin definition currently fits more with the IEEE definition of *data agency* (EAD, 2019) - this however is splitting hairs, as *privacy* and *agency* in the opinion of this report author, are two sides of the same coin.

It is worth mentioning that Professor Westin's book "Privacy and Freedom" (Westin, 1967), written under the auspices of the Special Committee on Science and Law of the Association of the Bar of the City of New York, is widely acknowledged as pioneering in worldwide privacy movements as well as privacy legislation in the United States. His proclamation that privacy provides individuals and groups in society " … *with a preservation of autonomy, a release from role-playing, a time for self-evaluation and for protected communication* … ", though initially contentious at the time of publication, is now widely accepted as elementary and basic to good privacy policy development.

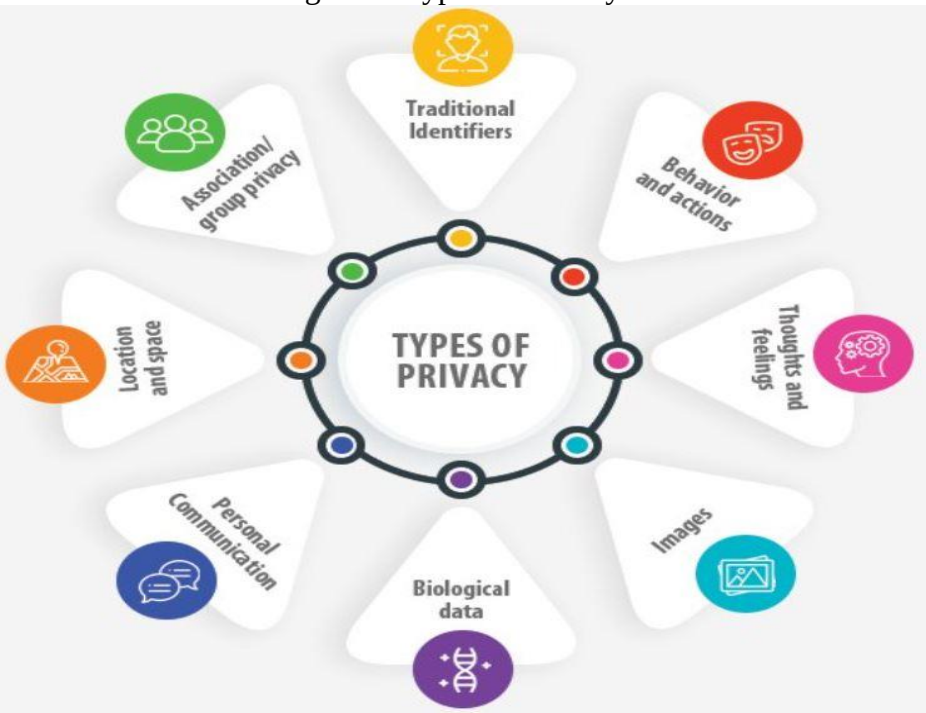
In the last couple of decades of rapid digital technological advancement, the definitions and implications of privacy, just as personal data, has also evolved quite a lot. In 2008 the author Daniel Solove described privacy as a " … *concept in disarray* … " (Solove, 2008). He argues rather controversially that the definition and remit of privacy was becoming too wide and encompassing, and goes on to list a number of things/concepts which he describes as too "sweeping". This report author completely disagrees – every concept in Solove's list is intrinsic to good privacy. Solove argues further that the determination of privacy ought to be based not on individual rights but on its importance to society. It is however the view of this report author that since society requires individuals as its basic building blocks, and individuals by their very nature require privacy to thrive, Solove's argument is at best half

baked. This report author concedes nonetheless that in situations where a known convicted criminal poses a danger to others, the privacy of the criminal can be placed lower in the order of considerations.

Current notions of privacy, though incorporating a wide range of concepts, by and large seem to converge on a set of few widely acceptable concepts. In January 2012 when the EU Commission published its proposals for a European data protection framework (a forerunner of the eventual GDPR), it identified seven types of privacy (Gutwirth *et al*, 2013). The 7 types are presented, together with an additional one of "traditional identifiers", in Figure 1.

While the "2022 Global Threat Report" by CrowdStrike identifies three types of privacy as *accessibility privacy*, *decisional privacy*, and *informational privacy* (CrowdStrike, 2022), these 3 broad types incorporate much of the 7 identified in Gutwirth *et al* 2013.

Figure 1: Types of Privacy



Reproduced from Deloitte Infographic by Antonio Grasso

It is also observed from the literature that in the USA, while federal attitude to personal data, privacy and safeguards can at best be described as patchy, some individual states have a well-defined and well-catalogued approach especially the state of California with its California Privacy Rights Act of 2020 (California, 2020).

Current debates on data protection and privacy safeguards

Although there is universal consensus on the need for better data safeguarding protocols, current debates revolve around the extent to which access to personal data should be balanced with the need for using authentic population data for societal good, for example large datasets of genomic data for medical and pharmaceutical research, considering the vast untapped potential of powerful machine and deep learning methods. Chloé-Agathe Azencott (Azencott, 2018), writes in the *Philosophical Transactions of the Royal Society* that to enable large

numbers of researchers to access genomic data, cryptographic frameworks such as homomorphic encryption (a form of encrypted database that enables users to perform computations on its encrypted data without first decrypting it) must be deployed. She asserts that technical developments in this emerging field should be accelerated to address current limitations in data access.

This author sides with her argument that cryptographic solutions would enable the removal of stifling and sclerotic "permission granting authorities" and thus give access to more high calibre researchers in medical and health sciences, without compromising privacy.

It is interesting to note that the literature contains, even if in the minority, authors that have a more relaxed attitude to privacy and safeguarding, sometimes alarmingly so. Lunshof *et al* (2008) and also Ball *et al* (2012), on the issue of using genomic data for medical/health research, take the view that " … *another approach is to somewhat give up on the notion of privacy, by informing study participants that, although appropriate measures will be taken to that effect, their privacy cannot be guaranteed …* ". On this, this report author takes a contrary view, which is that under no circumstance should the notion of privacy be given up, and that such views from such authors are irresponsibly cavalier.

In September 2021, the anticipated launch of the GP Data Sharing scheme in England, also known as the General Practice Data for Planning and Research (GPDPR), was postponed. Initially buried in an obscure government website, the scheme was described as a new framework with improvements for creating and managing a central NHS digital database from GP records in England. It is clear that a central database of this kind would enable valuable life-saving insights from longitudinal health data through modern machine and deep learning methods. The reason for the postponement – more than one million patients had opted out the month before launch, with increasing numbers opting out daily. The reason for the mass opt-out – a palpable absence of clarity and communication about the scheme, coupled to the perception that the government was "bouncing" (i.e. surreptitiously forcing) people into the scheme.

This incident is a classic lesson in what can happen when safeguarding reassurances are not given to users of any system that requires some level of voluntary participation. Instead of the success of a well-meaning and obviously beneficial scheme, the authorities presided over an exponentially growing groundswell of conspiracy theories simply by taking transparency in safeguarding for granted.

Professor Chris Holmes is Programme Director for Health and Medical Sciences at The Alan Turing Institute (TATI). In his published blog on the TATI website on "Why building public trust is key" regarding safeguarding, he identifies key principles and elements that need to be in place, among them " … *clearly stated principles for access to data, including transparency of its use* … " and " … *public and patient involvement in all aspects of analysis* … ". He states further that Turing ethics researchers argue " … *that data safety regulations, such as ISO 27001 and other data safe haven certifications, should be published and subject to random audit. Also, all organisations having such access should offer transparent and fair recompense in the event of data breaches* … ". Professor Holmes's pronouncements are typical of the current state of debate among Ethicists as well as AI professionals, and this report author sides with these sentiments.

Section B

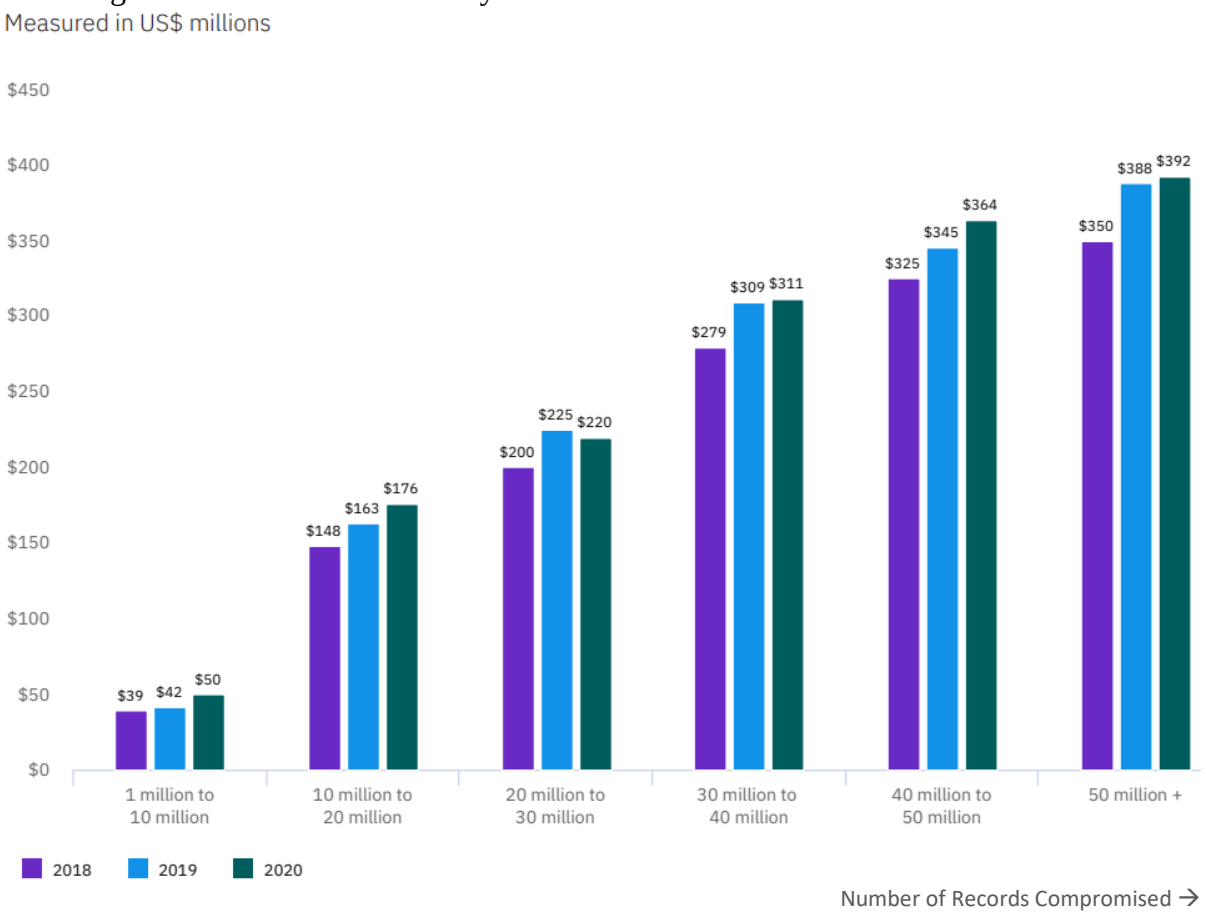
Research and Discussion

Data Breach: What Is It?

A data breach is said to have occurred when information in the form of data, or any other form, falls into the hands of person(s) not supposed to have the information. Mostly breaches occur all the time but only become news when large organisations are hacked. It is estimated that up to 85% of data breaches are caused by the human element (human error or deliberate attack) rather than by system glitches (ISO, 2020). Grey areas do exist in the mainstream definitions of data breach, for example a trusted former employee whose access to sensitive data is not rescinded months after they leave their post.

Data breaches have very serious implications, not least the loss of privacy – medical, business, association, intellectual property, or other data. A good barometer of the seriousness of data breach is the monetary cost to individuals and organisations. Cost is measured by a summation of activities such as detection and forensic incident response, lost business and revenue, notification of data subjects, data protection regulators and other third parties, helping and compensating victims of a breach, and paying regulatory fines. Figure 2 shows a year-on-year increase in monetary cost as well as number of records lost in data breaches for the last few years.

Figure 2: Variation of Monetary Cost with Number of Records in Data Breaches



Reproduced from Cost of Data Breach Report 2020, IBM Security

Data Breaches: Why They Happen

Data breaches happen for a variety of reasons, from sabotage to acquiring information about other(s) to acquiring financial benefit. The reason and/or mechanism whereby data or information "falls" into the wrong hands can broadly be divided into two:

1. Passive or careless custody on the part of the rightful owners, i.e. loss.
2. Active or orchestrated probing on the part of the wrongful acquirers, i.e. theft.

A tentative third reason/mechanism is

3. Deliberate exfiltration of data by an employee or insider for the purpose of whistle-blowing, or for the perception of addressing a grievance, i.e. leak.

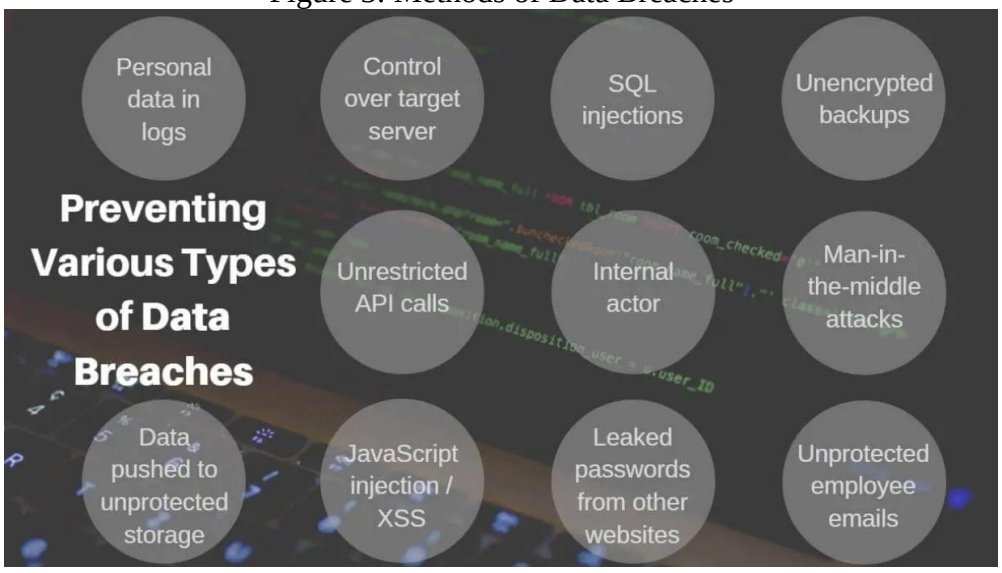
Loss of information can occur through accidental misplacement of hardware, for example the occasional but increasingly regular newspaper reports of government officials or civil servants leaving a laptop or a flash drive (USB stick) on a train. Loss can also occur when networks are not properly secured, thereby presenting themselves as easy targets for malicious network sniffers. Loss can also occur when IT systems are not properly configured, thereby leading to inadvertent routing of data to unintended recipients.

Theft of information occurs when an individual, group of individuals, or an organisation (including state intelligence actors) purposefully targets another individual or organisation and penetrates their information systems through phishing, social engineering, zero-day exploit of third party software, or backdoor exploits. The reason for theft is by far for financial gain, for example selling PII on the dark web or demanding ransom for returning data. Other reasons include enterprise competitors trying to steal trade secrets, and also nation-states spying on one another. It can also be due to simple debased voyeurism.

Information or data leaks occur, as previously said, due to an employee or insider turning into a whistle-blower, or a disgruntled employee with a grievance seeking to hurt their employers.

Figure 3 shows some of the various methods and means through which data breaches occur.

Figure 3: Methods of Data Breaches



Reproduced from LogSentinel

Critical Issues in the Marriott Case

While the motive for the intruder who breached the Marriott IT systems is not known for certain, it is believed actors working on behalf of the Chinese government conducted the hack for intelligence-gathering (Hotel Tech Report, January 2022). It is generally accepted that even if the breach was somewhat inevitable, it occurred through negligence on the part of Marriott/Starwood to apply due diligence in securing their IT systems. It is also generally accepted that Marriot ought to have discovered the breach much sooner than it did.

In relative context, the Marriott case, infamous for its scale, is actually not the worst case of known data breaches as it has been surpassed by others. The Marriott incident compromised the records of some 5.2 million individuals and cost the hotel conglomerate an estimated £35 million overall (ICO fine £18.4 million). In May 2020 EasyJet made public the loss of 9 million customer records which to date has already cost the airline an estimated £36 million (ICO fine £27.7 million) with more costs yet to come, i.e. a £2,000 per customer lawsuit is still pending. Also in 2020 Microsoft announced the exposure of 250 million records which has so far cost the technology giant over £1 billion with more cost yet to come, and in April 2021 it became known that Facebook had compromised the records of some 500 million users and has to date cost Facebook an estimated £1.5 billion with more costs yet to come.

Starwood, and by extension Marriott, were guilty of organisational cultural practices that bolstered the ease with which any bad actor could access so many guest records for such a long time, by persisting in the use of legacy IT infrastructure. The laying off of staff and hence the lack of personnel also prevented Marriott from quickly integrating newly acquired Starwood hotel properties into its own reservation system.

It is however noteworthy that none of the compromised guest records ended up for sale on the dark web, probably an indication that the hack was not for profit.

The contrast drawn by the Lesson 4 Lecture between the cases of Marriott and Mermaids (Transgender charity) is illuminating in terms of the balancing act the ICO performs when adjudicating breach culpability, liability, and issuing fines. The lecture pointed out that while Marriott had systems in place and were generally more cybersecurity aware, Mermaids did not have any cybersecurity defences, Mermaids staff were untrained in cybersecurity, did not have a savvy Data Controller, and ought to have applied a lot more due diligence in their cybersecurity posture. In this, this author agrees with both the lecture content and the ICO. It might be noted that while the Marriott breach was mainly about personal data, the Mermaids breach was more about sensitive data.

This author is in agreement with the way the ICO decides the amount of fines to companies or organisations that fall foul of data breaches. It takes into consideration variables such as the scale of the breach (i.e. number of records compromised) and the type of data compromised. It also considers mitigating factors such as not deriving any financial benefit from the breach, being a first offence, the breach being negligent but not intentional, and extending full cooperation to the ICO with respect to the latter's investigation. This can be seen in the wording of the Monetary Penalty Notices the ICO issued to Marriott (ICO, October 2020) and to Mermaids (ICO, July 2021), in that although Mermaids were more negligent and were more harshly criticised by the ICO, they received a monetary fine of just £25,000 compared to Marriott's fine of £18.4 million. This is mainly due to the scale of the breach, i.e. the number of records compromised. It may be that the *charity* status of

Mermaids compared to the *hotels conglomerate* status of Marriott might also have been considered by the ICO.

This author's major disagreement with the ICO is only in its exoneration of Accenture and also SecureWorks (Brewster, 2018) from liability. As third party security contractor and vendor respectively contracted to administer the IT systems of Starwood and later of Marriott after the acquisition of Starwood, both Accenture and SecureWorks are at least partially responsible for the negligence that enabled an intruder to instal code granting the intruder continuous access. As partial Data Processors for the Controller (Starwood, and later Marriott), Accenture and SecureWorks share in the duty of due diligence that would have enabled detecting the breach much earlier than it did. The ICO should therefore have issued appropriate fines for both Accenture and SecureWorks as well.

It is this author's opinion that Marriott's culpability can be assuaged by the fact that the method used to infiltrate Starwood's IT system is hard to defend against. i.e. phishing email where, even with a highly trained cybersecurity aware staff, clicking a link in a carefully planted bogus email is an easy mistake to make. If this is coupled to the high probability that the hackers were Chinese state actors with resources on the level of a modern nation state – as this author's DPO interviewee as well as a good number of published literature suspect – then Starwood stood little chance of preventing the actual infiltration. What Starwood, Marriot and Accenture should have done subsequent to the hack in detecting it earlier is a different matter, as each of them could have done more. This author also agrees with the DPO interviewee that following Starwood's acquisition by Marriott, the legacy IT system at Starwood should have been upgraded and integrated in the Marriot IT infrastructure more speedily.

On the issue of cookie consent, the UK has taken a backward step after Brexit and UK's departure from the EU GDPR. It has been noted, not just by this author but by other commentators too, that the privacy notices presented by websites to UK residents after Brexit is trickier to navigate and more deceptive than pre-Brexit when UK was fully part of the EU GDPR.

This author concurs with the Lesson 4 Lecture opinion that " … *having legislations is not enough, following them diligently is important* … " (Lesson 4 Lecture, 2022).

In the light of this research, it is recommended that companies and organisations take an uncompromising approach when implementing the following reasonable mitigation actions:

1. Encryption at rest.
2. Encryption in transit.
3. Multi- or 2-factor authentication (MFA and 2-FA respectively).
4. Remote deactivation.
5. Regular systems audit for early detection in case of breach.
6. High cybersecurity awareness and training for all employees.
7. Highly qualified and experienced cybersecurity team/department, regularly refreshed with new talent.

Relation to GDPR and UK Data Ethics Framework Principles
From the literature and particularly from the ICO's Monetary Penalty Notice to Marriott, it is obvious Marriott broke the following articles relating to GDPR and the UK Data Ethics Framework Principles:

1. Under Article 5(1)(f) of the GDPR, Marriott should have processed personal data in a manner that ensured appropriate security, and protected it against unauthorised and unlawful processing. Marriott's Data Controller failed in this duty.

2. Under Article 32 of the GDPR, Marriott should have taken into account the state of the art, the scope, context, costs, and purposes of processing the personal data as well as the risks involved thereof and should therefore have taken appropriate technical and organisational measures such as encryption, multi-factor authentication, testing and evaluating their systems to ensure the safety of personal data. In this also Marriott failed.

Relation to ICO Data Sharing Code & Data Protection Act 2018
From the literature and also from the ICO's Monetary Penalty Notice to Marriott, it is clear Marriott contravened the following ICO Data Sharing Code & DPA 2018:

1. Section 149(2) of DPA 2018

2. Section 155(1)(a) of DPA 2018

3. Section 155(2) to (4) of DPA 2018

Based on these clauses the ICO calculated and imposed a fine on Marriott through powers granted it under GDPR Article 83(1) and (2).

Section C

Conclusions and Recommendations

Privacy by its very nature has, through the ages, been disputed and contested, and will continue to be in a state of flux by virtue of changing social and technological advancements. The now very advanced nation of China adopts a policy to the effect that for the sake of societal good, privacy must be relegated to an afterthought. There are many others in our midst even in the geopolitical West who also subscribe to this view. This author disagrees vehemently, and is of the opinion that privacy and personal data are inherently and manifestly requisite for sound human development, and that in the formation of societies and other social constructs, it is the basis of maintaining some individuality that makes us human. This philosophy of individuals who participate in society and other social constructs willingly is borne out by Darwinian evolution (Darwin, 1859), in that human societies developed division and specialisation of labour and rewards, but did not go on to fully fledged herd or swarm communities like ants, bees, crabs or locusts.

It is in this tradition that this author agrees with the findings and sentiments expressed subsequent to TATI workshop in the publication on the theme "The ethical impact of data science" (Mulligan et al, 2016). Of the 3 key areas of research identified as posing ethical challenges to the implications and impact of data science, Mulligan *et al* distil as key the implementation of a large-scale ethical framework, and not on the reliance of narrow or ad hoc approaches. They point to a rich 30-year legacy of computer and information ethics that should be built on in response to the growth of digital technologies. Their conclusion to the effect that " … *striking a robust balance between enabling innovation in data science technology, and respecting privacy and human rights will not be an easy or simple task. But the alternative, failing to advance both the ethics and the science of data, would have regrettable consequences* … ", is in this author's opinion a statement of fact that is not contestable.

Much as this author would like to recommend accelerated funding into homomorphic encryption research due to its capacity to enable the unlocking of insights into health data, this is not a matter for the ICO but for governments and funding bodies.

Given that the Marriot breach, as well as other notorious hacks, could have been mitigated by the simple implementation of data *encryption at rest* with encryption-decryption keys stored on a different system, it is recommended to the ICO that both *encryption at rest* and *encryption in transit* with alternative or separate key storage be made mandatory by law instead of these being guidelines and recommendations. In the light of this research which uncovered something cybersecurity professionals have always known, the ICO might also be invited to consider making the storage of encryption/decryption keys on the same system as the data it encrypts/decrypts a criminal offence.

It is obvious, from my interview with the DPO of a Technology Startup, that legacy systems working concurrently with new or updated infrastructure always presents a menace. Here it is recommended that the ICO not to make a mandatory requirement just yet but to make it a strong recommendation in UK GDPR and in any update of the UK Data Protection Act that the data in legacy systems are transferred within 6 months of company acquisitions and mergers.

The often used phrase "*appropriate technical and organisational measures*" by the ICO must be set out and spelled out in listed detail, point by point, what this phrase entails. This will of course require regular updates given the current and anticipated pace of technological development. The ICO should also have a clear metric or measure for "intrusivity" (i.e. intrusiveness) with clear demarcations of different levels of how *personal* and/or *sensitive* any compromised data is, and factor that into the monetary penalty it issues. Granted that the level of compromise of a system is often not clear for a while after discovery of a hack (which to a greater extent is due to prevarication than to incident response forensics), this author concedes that this would not be easy.

The final recommendation to the ICO is that, as much as possible, it should have a proactive department or wing to recommend and legislate against anticipated threats. It should not restrict itself to shutting stable doors when the horses are already miles away. A poignant example – at the time of writing this report, the *metaverse* is on the verge of becoming massive. Immersive virtual worlds are potentially the next paradigm shift in how technology is served and consumed, not necessarily with the current tiny headsets but with other developments currently in drawing board, pilot, and concept stages. These would deliver experiences like shopping, work-from-home work meetings, university lectures, GP appointments, and other activities in a completely different way. Scouting the literature shows anticipation of the potential problems among some ethicists (Agerskov, 2021), (Creativepool, 2022). Governments and regulatory authorities appear to be waiting for the next series of catastrophes and scandals before being jolted into action. Although it is not easy to anticipate the direction of technological travel, it should be clear to bodies such as the ICO that the metaverse is very much the next frontier.

All these require that a very careful and considered balancing act is performed so as not to stifle innovation often from small ambitious tech businesses who do not have the resources to deal with reams of regulation and bureaucracy from on high. Perhaps regulatory requirements could be calibrated according to an enterprise's number of employees and annual turnover, in addition to the number of personal records on its IT systems.

With the ascendancy of data science and AI however, the future is brighter, if humankind chooses to use it for good rather than evil.

References

1. Afifi-Sabet, Keumars, (2020), Marriott data breach exposes personal data of 5.2 million guests, *IT Pro*, [online]: https://www.itpro.com/security/data-breaches/355173/Marriottt-hit-by-data-breach-exposing-personal-data-of-52-million

2. Agerskov, S., (2021), The Metaverse – A Dystopian Future?, *Data Ethics*, [online]: https://dataethics.eu/the-metaverse-a-dystopian-future/

3. Azencott, Chloé-Agathe, (2018), Machine learning and genomics: precision medicine versus patient privacy, *Phil. Trans. R. Soc*, **A 376**, 20170350, [online]: http://doi.org/10.1098/rsta.2017.0350

4. Ball, M.P. et al., (2012), A public resource facilitating clinical use of genomes, *Proc. Natl Acad. Sci. USA*, **109**, 11 920–11 927., [online]: https://www.pnas.org/doi/full/10.1073/pnas.1201904109

5. Brewster, Thomas, (2018), Revealed: Marriott's 500 Million Hack Came After A String Of Security Breaches, *Forbes*, [online]: https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/?sh=448ed45c546f

6. California, (2020), The California Privacy Rights Act of 2020, [online]: https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

7. Clarke, Roger, (2006), What's 'Privacy?, *Australian Law Reform Commission Workshop*, July 2006, [online]: http://www.rogerclarke.com/DV/Privacy.html

8. Creativepool Editorial, (2022), Privacy has changed: How can brands keep customers safe in the metaverse?, *Creativepool Magazine*, [online]: https://creativepool.com/magazine/workshop/privacy-has-changed-how-can-brands-keep-customers-safe-in-the-metaverse.26719

9. CrowdStrike, (2022), Global Threat Report, (2022), *In-depth analysis of the most significant cybersecurity events and trends of 2021*, [online}: https://go.crowdstrike.com/global-threat-report-2022.html?utm_source=goog&utm_medium=dis&utm_campaign=globalthreatreport&utm_term=psp_ci_itdm&utm_content=gtr22_v1_uki_en_rda&gclid=EAIaIQobChMI1auIxJCj9wIV_wT5AB09BQBfEAEYASAAEgJ7__D_BwE

10. Darwin, Charles, (1859), On the Origin of Species by Means of Natural Selection, [online}: http://darwin-online.org.uk/converted/pdf/1861_OriginNY_F382.pdf

11. EAD, (2019), Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, Institute of Electrical and Electronics Engineers (IEEE), pp. 23-24, [online]: https://ethicsinaction.ieee.org/wp-content/uploads/ead1e.pdf

12. Friedewald, Michael, Finn, Rachel, and Wright, David, (2013), Seven Types of Privacy, *PRESCIENT project*, pp. 3-32, [online]: https://www.researchgate.net/publication/258892458_Seven_Types_of_Privacy

13. Fruhlinger, Josh, (2020), Marriott data breach FAQ: How did it happen and what was the impact?, *CSO Online*, [online]: https://www.csoonline.com/article/3441220/Marriottt-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

14. Gutwirth, S., Leenes, R., Hert, P., and Poullet, Y., (2013), European Data Protection: Coming of Age, *PRESCIENT project*, pp. 59 – 84, [online]: https://www.researchgate.net/publication/278636601_European_Data_Protection_Coming_of_Age

15. Hotel Tech Report, (January 2022), *Marriott Data Breach - What Really Happened* [online]: https://hoteltechreport.com/news/Marriottt-data-breach#:~:text=Background%3A%20Marriottt%20Data%20Breach%202014,database%20for%20Marriottt's%20Starwood%20brands

16. Hut 6 Security Limited, (2021), *Data Protection Act's Eight Principles*, [online]: https://www.hutsix.io/what-are-the-eight-principles-of-the-data-protection-act/

17. IBM Security, (2020), Cost of Data Breach Report, [online]: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

18. ICO, (2021), *Guide to the General Data Protection Regulation (GDPR)*, pp. 10 – 13, [online]: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf

19. ICO, (July 2021), Mermaids Penalty Notice, [online]: https://ico.org.uk/media/action-weve-taken/mpns/2620171/mermaids-mpn-20210705.pdf

20. ICO, (October 2020), Marriott Penalty Notice, [online]: https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf

21. ISO, (2020), 2020 in Review, *International Organisation for Standards Annual Report*, [online]: https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27040:ed-1:v1:en

22. Lunshof, J.E., Chadwick, R., Vorhaus, D.B., Church, G.M., (2008), From genetic privacy to open consent, *Nat. Rev. Genet.*, **9**, 406–411. [online]: https://www.nature.com/articles/nrg2360

23. Mulligan Deirdre K., Koopman Colin and Doty Nick, (2016), Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy, *Phil. Trans. R. Soc.*, **A 374**, 20160118, [online]:
    1. https://royalsocietypublishing.org/doi/10.1098/rsta.2016.0118 ,
    2. https://www.turing.ac.uk/news/published-today-new-research-ethical-impact-data-science

24. Lesson Lecture, (2022).

25. Lesson Lecture notes, (2022).

26. Solove, Daniel J. , (2008), Understanding Privacy, *Cambridge Massachusetts: Harvard University Press*, p. 1 and pp. 67 – 69.

27. The California Privacy Rights Act of 2020, (2020), [online]: https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf

28. UK DPA, (1998), Data Protection Act 1998, National Archives, [online]: https://www.legislation.gov.uk/ukpga/1998/29/contents

29. UK DPA, (2018), *Data Protection Act 2018*, [online]: https://www.gov.uk/data-protection/print

30. UK GDPR, (2021), [online]: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/

31. Wan, Z., Vorobeychik, Y., Xia W., Clayton E.W., Kantarcioglu M., and Malin B., (2017), Expanding access to large-scale genomic data while promoting privacy: a game theoretic approach, *Am. J. Hum. Genet*., **100**, 316–322, [online]: https://www.sciencedirect.com/science/article/pii/S0002929716305262

32. Warren, Samuel D., Brandeis, Louis D., (1890), The Right to Privacy, *Harvard Law Review*, **4**, (5), pp. 193-220, [online]: https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/hlr4&id=206&men_tab=srchresults

33. Westin, Alan F., (1967), Privacy and Freedom, *Atheneum. pp. 6 - 8.*

Appendices

Appendix 1. The 6 (or 7) principles of the UK Data Protection Act 2018 (UK DPA, 2018)

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

❖ a 7th principle of Accountability, currently not visible under the UK DPA 2018, requires " … *organisations to take responsibility for the personal data being handled and their compliance with the other six principles. Appropriate measures and records are also required to be in place as to demonstrate compliance* … " (Hut 6, 2021).

Appendix 2. The 9 data constituents of *sensitive information* of UK DPA

1. race
2. ethnic background
3. political opinions
4. religious beliefs
5. trade union membership
6. genetics
7. biometrics (where used for identification)
8. health
9. sex life or orientation

Appendix 3. Transcription of interview in April 2022 with DPO of Tech Startup

Interviewer (this author): redacted (opening greetings, salutations, and chat).

Interviewee (DPO): redacted (opening greetings, salutations, and chat).

Q1: What is the current state of data protection and privacy safeguards in UK, and in the wider world?

A1: It is an evolving landscape, and I am happy to say it is being taken more seriously as time goes by, both in the UK and worldwide. There are obviously pockets of regions in the wider world where it could be better, but the general trend is for the better.

Q2: What is your opinion of the Marriott breach and how the ICO dealt with?

A2: Oh, where do I start? There's a lot published online on this matter which I believe you've already found so no need to labour the points. OK, overall I think the ICO decision in the end was the right one. And the fine also.

Q3: Who in your opinion hacked the Marriott system?

A3: Actual evidence of attribution in cases like this can be hard to come by, but there is sufficient fingerprint evidence for me personally to think contract hackers working for the Chinese government were responsible, but I can't be 100%.

Q4: Do you think there was more Marriot could have done?

A4: Absolutely. They made a number of mistakes, I'll just mention the most serious ones which incidentally were the most basic. First of all Marriot made a mistake that baffles most computer security professionals. Basic security 101 is you do not keep encryption keys on the same system that the data is stored. Marriot appears to have done just that. Their other serious mistake is something that old school organisations don't seem to have grasped yet, but Startups are very aware of and avoid, which is that legacy data must be safely transferred asap and the legacy system itself decommissioned asap.

Q5: Do you think the ICO has enough power? Should it have more or less power than it currently has?

A5: Hmm, that's a hard one. I would say its current powers are about enough, just right. I recently read that MPs (i.e. Members of Parliament) are considering giving ICO more powers. I am always wary of bureaucrats wielding more and more powers. It is never good for smaller businesses, and for businesses that thrive on being inventive.

Q6: I have seen from the literature that in the Marriott case, the data did not end up being sold on the dark web. In your opinion, what did the hackers do with data then?

A6: Hah, that's a good and an even harder question. I really would have to pass on this one, as anything I say would be pure speculation. There are some sources online though that you can check out, but again they are more speculation than fact. I don't think anybody knows that for sure.

Q7: What is your takeaway message with regard to the Marriot case?

A7: Well, 3 words really, and its "monitor, monitor, monitor". When it comes to security you cannot over-monitor a system. And always assume you've been hacked even if there is no evidence, and work from there by monitoring infrastructure and systems configuration in such a way that lateral transfer and lateral access is as tight as possible, and to detect anything unusual. I would also add high employee security training and awareness.

Q8: Many thanks for your time and insights today. Have a good day. Bye.

A8: You're welcome. Take care and stay in touch. Bye.