



# AN INVESTIGATION OF GENDER BIAS AND GDPR IN RELATION TO MARRIOTT HOTELS

Elliot Linsey

ETHICS, REGULATION AND LAW IN ADVANCED DIGITAL  
INFORMATION PROCESSING AND DECISION MAKING  
ECS7025P

MSc FT Data Science and Artificial Intelligence (Conv)

Submission Date: 01/05/2022  
Word Count: 4131



## Table of Contents

<i>List of Abbreviations and Glossary .....</i>	<i>2</i>
<i>Executive Summary .....</i>	<i>3</i>
<i>Literature review .....</i>	<i>3</i>
<i>Marriott Case .....</i>	<i>5</i>
Critical Issue: .....	5
Interview with Expert.....	6
<i>Recommendations .....</i>	<i>8</i>
<i>Conclusion .....</i>	<i>9</i>
<i>Bibliography .....</i>	<i>10</i>



## List of Abbreviations and Glossary

ICO: Information Commissioners Office

DPA: Data Protection Act

GDPR: General Data Protection Regulation

EU: European Union

UK: United Kingdom



## Executive Summary


Machine learning is a rapidly evolving field of study with potentially limitless application. This report identifies areas of gender bias within machine learning due to old training data that does not reflect current values, as well as the different forms this imbalance can take such as discounting female achievements or enforcing stereotypical gender roles. It also examines the potential for misogyny within the teams working on machine learning projects and the methods being proposed to reduce the impact of gender bias on AI development. Furthermore, the report investigates the Marriott data breach case of 2018 (BBC 2020) and identifies key issues such as the type and amount of data lost. An expert is then introduced who provides an analytical commentary on the case as well as general issues with the EU GDPR (EU GDPR, 2016) such as anonymisation, cloud storage, and how these issues affect the consumer. Recommendations regarding the Marriott case and GDPR are presented with suggestions such as higher levels of data protection protocol, more effective fines, clearer guidelines and more stringent data sharing procedures.

## Literature review

This literature review shall be exploring the notion of gender bias within machine learning and AI algorithms. At the present day, there is clear evidence of gender bias infiltrating these systems from a multitude of angles. These include biased training data, a lack of diversity within AI development, economic factors, and potential inbuilt misogyny within the social setting. This bias causes negative effects to the female sex by potentially penalising them within applications or work-related roles as well as categorising them in different and demeaning manners compared to males. A large amount of research done in this subject has been led by female researchers who are best able to identify and relate to the issues that gender bias causes within AI as well as the STEM field in general.

“A computer program is said to learn from experience  $E$  with respect to some class of tasks  $T$  and performance measure  $P$ , if its performance at tasks in  $T$ , as measured by  $P$ , improves with experience  $E$ .” (Tom Mitchell, 1994). This quote is used to summarise the process of a machine learning algorithm, and although advancements have been made with new techniques and methods, the general formula has stayed the same. The issue that is currently being faced by machine learning scientists and AI practitioners is to do with the experience section of the above quote, where imbalanced datasets that do not contain the full range of experience to learn from can lead to “bias in machine learning algorithms that have troubling implications and deleterious consequences” (Weiss et al, 2018)

Due to the material within older corpora that machine learning algorithms are being trained on, gender bias has been observed within current algorithms due to the outdated ways of referring to men and women (Leavy, 2018). This is due to the heavily male-centric way of thinking and writing within periods such as the 50s and 60s, with women being referred to with far more appearance-based descriptions and metaphors compared to men, who are described according to accomplishment. For example, women are commonly referred to as dessert items which can be demeaning, such as ‘cheesecake’, ‘honeybuns’, ‘tart’ (Hines, 1999). This form of bias is known as representation bias, where associations between concepts and gender are embedded within AI systems due to material it has been trained on. The other form of bias is known as allocation bias, where algorithms reward the majority



gender within documents (Crawford, 2017). This form of gender bias has been observed with the Amazon company resumé rating system, it started to penalise those that contained vocabulary such as “women’s chess captain,” and those that attended all-women colleges (Dastin, 2018). This is due to the vast majority of previous successful applicants that the algorithm was trained on being male, therefore it would reward those resumé that were similar to the ones that it had been told were previously successful and discount the female resumé.

Whilst the data these algorithms are being trained on may be problematic, another influencing factor on the gender bias seen within machine learning could also be related to the programmers and developers themselves (Nadeem et al, 2020). Within AI development the male perspective has been dominant through sheer force of numbers. An example of this type of gender bias can be observed with the Github platform, where women’s acceptance rates are higher for open-source projects only when they are not openly identifiable as women (Terrell et al, 2017). There are more initiatives being developed to encourage and support female entrants into the field, however this is only a first step into eliminating gender bias (Parsheera, 2018). Successive measures such as cross-disciplinary teams, bias identification methods and fairness measures being built into evaluation metrics could be the next stepping stone for reducing the impact of gender bias during AI development. Whilst these are excellent goals to strive for, the fact of the matter is that a lot of the data being used to train AI models still uses heavily biased terms, such as ‘chairman’ instead of ‘chairperson’. The most difficult step would be correcting this training data itself. Education could be implemented to work with the current generation of digital content producers but also to influence the next generations to use more gender-neutral terms in their creations.

An issue with implementing these changes to the development of AI is that of economic factors, as well as research capability. Technology is designed and created by engineers, but the actual reason for its creation is down to socio-political factors or profit motivation (Wang, 2020). Due to this, there would need to be an active involvement by businesses and governments to tackle the effects of gender bias. Some governments have already stated their desire to be involved more prominently in specific areas of AI development, such as the UK wishing to play a greater role in the ethics element of AI creation (House of Lords, 2018). Currently, countries such as the UK are focusing on creating ethical frameworks for the development of AI (such as the UK Data Ethics Framework) and enforceable law (such as the EU General Data Protection and Regulation Act). As these become more widely accepted companies will have clearer instruction and guidance on how to best avoid not only gender bias but also consider ethical considerations and address them within their products (UK Data Ethics, 2020).

The removal of gender bias within AI systems is still a work in progress. However, as seen, a number of issues must be addressed. These being the material within older corpora containing inbuilt bias and male-centric viewpoints, as well as current AI training techniques rewarding majority classes. Another being the male dominated field of AI development which can have an unconscious yet negative impact on female representation within AI products. Finally, to implement these changes, governments and businesses need to be involved and make an active effort to combat gender bias.



## Marriott Case

According to the UK Information Commissioners Office (ICO), a personal data breach is the “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.” (ICO, 2018). There are a number of reasons why a data breach may occur, with the majority of them not containing explicit malicious intent by bad actors. A number of examples from the ICO itself contain scenarios such as:

- Sending an email with sensitive information to the wrong recipient
- Misplacing a laptop or thumb drive with sensitive data
- Deletion or alteration of data
- An unauthorised third-party gaining access to data
- An inadequate response or data protection by the data controller


The Marriott case is connected to the last 2 of these examples, due to the fact that the data was breached by a third party and the company had inadequate protection in place. In terms of Marriott’s fault in relation to its protection policy, the intrusion was actually put into the Starwood Resorts system in 2014. Marriott subsequently purchased Starwood in 2016 and did not notice the intrusion until 2018, giving the attackers another two years to potentially steal data (BBC, 2020). Due to Marriott being the data controller under the definition of section 6 of DPA, they have been found at fault in their ability to adequately protect personal data as required by Article 32 of GDPR as well as Article 5(1)(f) (EU GDPR, 2016).

### Critical Issue:

The most critical issue of this data breach was the amount of data that the attackers had access to, with an estimated 339 million users potentially at risk from the breach (BBC, 2020). Looking at the Marriott hotels current data collection standards, we can see the vast amount of information that was vulnerable during the breach period (Marriott, 2021):

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Financial information (such as credit and debit card number or other payment data)
- Language preference
- Date and place of birth
- Nationality, passport, visa, or other government-issued identification data
- Important dates: birthdays, anniversaries, and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details (for business-related bookings)
- Travel itinerary, tour group, or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

Data such as financial, passport, and visa information is extremely valuable and can cause devastating harm if put into the wrong hands. Not only this but clearly identifiable



information such as names, telephone numbers and addresses that are classified as personal data are also collected every time you make a booking. Due to the sensitivity of the data that Marriott holds, it is therefore an even greater example of negligence or mismanagement of data protection that allowed access to this amount and level of data. In response to this, the ICO was able to administer a fine of £18.4million under articles 83(1) and (2) of GDPR (ICO 2020), under the belief that it was a proportional response and would be effective in making Marriott increase its data security.


In relation to the UK Data Ethics Framework, the principle that relates most to this case would be that of accountability. This requires there to be effective governance and oversight for any data project, which Marriott hotels either were not able to or declined to provide. To further simplify this, Marriott were required to keep the data that they processed (EU GDPR, 2016, Article 4(2)) in a secure manner to prevent unauthorised actors from gaining access to it. Due to a data breach occurring, Marriott failed in this capacity and thus should be held accountable for its inaction in upholding data security protocol.

### Interview with Expert

From an interview with a person knowledgeable about this subject (henceforth referred to as the Expert), they bring up a number of points regarding data breaches, the nature of the data that Marriott was taking from customers as well as the limitations of UK GDPR and the future that UK GDPR is currently moving towards.

In regards to the data breach, the Expert mentions the fact that this exploit had been in the system for 4 years until it was discovered. You would expect during this time period that actions taken to both upgrade existing security and look for potentially infected systems would have been taken. Also, the fact that Marriott took over the original Starwood system and did not notice the malware suggests that they were not thorough in their takeover process and may not have been willing to make sure all systems were up to standard. The Expert attributes this seemingly lackadaisical approach to either ignorance of data standards and appropriate security measures, or possible negligence by Marriott hotels due to the fact that the Data Protection Act was updated in 2018 and they did not understand how it could affect them. However, when the exploit was discovered, Marriott hotels did act promptly in informing the ICO and performing damage control with its customers, including installing preventative security measures. It is unfortunate that it took a breach of this scale for a company of this size to revisit its security protocol and patch up holes in their system. Another point the Expert makes is how this was a 4-year long attack with the breach of 339 million users and Marriott hotels was fined £18.4million. On the surface this sounds like a large sum of money, however the Marriott International, Inc (that owns Marriott hotels) operates 30 brands internationally with a revenue of \$20billion in 2018 (Statista, 2022). To a corporate entity such as Marriott International this fine would barely create any lasting impact and may have been seen as a minor nuisance. It is certainly possible that Marriott were happy to not upgrade their system until forced to due to their knowledge that any fine enacted on them would not have any significant impact.

Another point to take into consideration is that Marriott likely profited from this data during the period. From the Marriott privacy policy, they state that they share your data not only with franchises within the Marriott group, but also third-party services such as airlines, car rental services, restaurants and promotional marketing companies that will target you based




on your data (Marriott, 2021). With this in mind, £18.4 million is likely dwarfed by the profit they made from selling their customers data during the time period.

Another point mentioned by the Expert was on the type of data declared vulnerable by Marriott hotels, and the data that Marriott collects and has access to as a whole. The official ICO report states that users may have had their “names, email addresses, phone numbers, unencrypted passport numbers, arrival/departure information, guests’ VIP status and loyalty programme membership number” compromised (ICO, 2020). However, as seen above within the privacy policy it is known that Marriott also collects information such as gender, employer, place of birth, as well as any data that is linked to social media accounts. This extraneous type of information could be used to access user accounts not connected with Marriott hotels, for instance, using place of birth to guess security questions and allowing the hacker access to even more sensitive data about an individual.

The Expert then moves on to more general issues with the GDPR. For one, the concept of anonymisation is currently being investigated in the context of data privacy and data consent (Esayas, 2015). When combined with other data, it is becoming far easier to identify individuals using supposedly anonymised data. This is because most processes that are classed as anonymisation are actually pseudonymisation. Anonymisation in this context is rendering certain information “non-personal” so that the subject cannot be re-identified. Therefore, this information can now be processed without the consent of the original user as it can no longer be used to identify a natural person, which would be illegal under GDPR (EU GDPR, 2016, Article 4(1)). Complete anonymisation of data is becoming more difficult with advances in technology (Keen 2020), and what most companies think of as anonymisation is actually pseudonymisation where they replace subject attributes with codes or replacement values. The Expert then states how this is very different from true anonymisation in the eyes of the law as pseudonymised data is far easier to identify natural individuals with. Therefore, companies that use this data are actually breaking GDPR by processing it (for its non-original purpose) under previously mentioned GDPR Article 4(1). In relation to the Marriott case, there does not appear to have been an attempt to anonymise or at least pseudonymise the data processed by the company which may have increased the ability of the attackers to identify or cause harm to the users.

In relation to data security, the Expert discusses how companies are starting to move their data storage and processing facilities to external companies (referred to as the cloud), such as Amazon and Google (Hashem et al, 2015). These cloud companies invest heavily in cybersecurity and data backups and therefore it should be harder to have a data breach or loss of data. However, this opens up a grey area within legislation and GDPR due to the user’s data rights and how they are potentially being signed over to third party companies, as well as the lack of legal provision to enforce policy within the cloud environment (Kshetri, 2013). It is unclear what cloud companies are allowed to do with processed data, in signing an agreement to process data for a company (such as Marriott) are they allowed to use it for purposes such as machine learning? How ethical is this on the user? Privacy agreements are already convoluted due to legal requirements (Cave, 2016) so the addition of another clause stating that a user’s data shall be stored with an external data provider is likely to be unnoticed. Whilst a user may initially consent to their data being used by the actual service provider (such as Marriott when booking a hotel and their other subsidiaries), you might not






expect your data to then be processed and used by a third-party company such as Google. In essence, by consenting for your data to be used by one company you are unknowingly consenting for it to be used by the cloud company that is actually storing the data. This leads into the Expert's next point, that GDPR is focused on protecting businesses and not consumers by placing too much responsibility on the individual for data protection (Layton, 2019). The GDPR is explicitly set out to provide guidance for businesses in how to handle data. What this results in is overly complicated privacy policies that the average consumer does not have time or knowledge to understand. Within this are ambiguities such as the length of time data can be stored, GDPR contains the storage limitation principle which requires companies to not keep data for longer than it is needed (EU GDPR, 2016, Article 5(1)(e)). This is open to abuse as it is difficult in some cases to define when data is no longer needed. For Marriott, they define it as "The length of time we have an ongoing relationship with you and provide the Services to you" (Marriott, 2021). This includes holding an account with them. From the consumer point of view, an individual may create an account and book a hotel stay with Marriott for a single trip, yet Marriott is well within its rights to hold that data about you indefinitely, as well as share and collect additional data to create an accurate profile of your behaviour for the foreseeable future.

The Expert brings up a final point for the future of GDPR within the UK and what direction our data privacy laws are being taken in. Firstly, it must be understood that the GDPR is a federated document within the EU (Pinsent Masons, 2013). This means that countries can have different rules and standards on how they enforce data protection under their Data Protection Authorities, for example the UK DPA is the ICO whereas the French DPA is the Commission Nationale de l'Information et des Libertés (CNIL). Due to the UK leaving the EU in 2020 due to Brexit, the UK GDPR is being rewritten to be less strict in line with the slogan "Build Back Better" (Afifi-Sabet, 2021). This rewrite is to encourage companies to store data within UK borders and attempt to address some of the issues raised within EU GDPR. Some of these relaxations include replacing Data Protection Officers with a "suitable individual" that does not have independent and regulatory role under previous EU GDPR. Record keeping requirements would also be removed and would be left to the businesses to determine under their own data privacy programme. The threshold for reporting a data breach would also be amended to reduce overreporting to the ICO which takes up time and resources (Gunn et al, 2021). These revisions highly reduce the amount of oversight required by companies to make sure they are keeping in line with current data laws and hence are very attractive. However, the UK currently holds adequacy status within the EU as a 'third country'. This means that personal data of EU citizens can be held in the UK only if the UK upholds equivalent levels of data protection to that of the EU (Sorensen, 2021). By relaxing the UK data protection standards, there is a risk of the UK losing this adequacy status and being unable to process personal data of EU citizens. To companies such as Marriott this could strike a serious blow and in the grand scheme of things actually hinder the UK's efforts to "Build Back Better".

## Recommendations

In terms of the Marriott case, a number of recommendations can be made. Firstly, when incorporating an external data source into your own (such as Starwood), a thorough analysis should be conducted to identify weak points and vulnerabilities or current malware. Secondly, routine sweeps of current infrastructure should occur as well as measures to check where



data is being sent to. Unknown or potentially exploitative behaviour should be flagged and followed up on. For recommendations to the ICO, the fine related to breaking data protection law should scale better in relation to the size of a company. For Marriott, the fine was £18.4million which equates to 0.092% of their revenue in 2018. This amount is not going to make companies of this size take serious notice of data protection which is even more dangerous as these are the companies that contain the most personal information about users. During the Covid-19 pandemic, travel companies such as Marriott were collecting health data such as vaccination status (NYTimes, 2021). While they may not be enforcing policy based on a customer's status, the potential for this health data to be shared is dangerous and may lead to information about religion and ethnicity as well as lead to possible discrimination. Clearer guidance should be enacted about what companies can and cannot do in relation to this type of data and whether they should be allowed to collect it in the first place. The ICO is the UK Data Protection Authority that has the ability to enforce legal recourse under the UK GDPR. An issue with enforcing GDPR is that some parts are potentially vague, such as the actual definition of personal data. Whilst it provides examples such as 'name', 'occupation', 'location', the extent to which these can be used to identify a natural person depends on the context of the data. For example, if you collect the name 'John Smith', this is not necessarily personal data due to the high numbers of people named 'John Smith'. However, when combined with an address, this information may be classified as personal data due to only one person named 'John Smith' living at this specific address. The ICO should provide better guidance on not only what type of data classes as personal data in regards to different contexts, but also on concepts such as anonymisation to provide a base level example that companies can follow (Irwin, 2022).

## Conclusion

As machine learning capabilities improve, we must recognise that our model will only provide a reflection of the data inputted to it. At this point in time, the greatest hinderance to removing gender bias within machine learning is the presence of outdated training data that our models are learned on. To combat gender bias in its entirety, we not only need to clean our training data of stereotypes and gender roles but also educate society on the harmful effects of invisible misogyny and promote methods, practices and guidelines that result in equity between the sexes. In analysing the Marriott case, there was the significant issue of the amount of data that the company had access to and the improper attitude to protecting it. Issues within the GDPR itself such as anonymisation, cloud storage and the less stringent future of UK GDPR are all areas that will affect consumers around Europe and the globe. A number of recommendations are suggested to combat some of the current issues with data protection, such as higher quality data checks, more effective fines, clearer guidelines on what constitutes 'personal data' and anonymisation. What must be stressed is the effect that big data can have on the individual. Within every record stored by companies such as Marriott is information that can have severe consequences if mishandled. Currently, GDPR is a step in the right direction, however it contains numerous grey areas that the legislation is struggling to fill. This leaves both companies and consumers in dangerous territory with the ability for negligent behaviour to take place a high and concerning possibility.



## Bibliography

ACLU, 2016. Predictive Policing Today: A Shared Statement of Civil Rights Concerns. Available at:

[https://www.aclu.org/sites/default/files/field\\_document/jointstatementpredictivepolicing17orgs.pdf](https://www.aclu.org/sites/default/files/field_document/jointstatementpredictivepolicing17orgs.pdf) [Accessed 24th February 2022]

BBC, (2020), Marriott Hotels fined £18.4m for data breach that hit millions. Available at: <https://www.bbc.co.uk/news/technology-54748843> [Accessed 14/04/2022]

Cave, B. (2016). Op-ed: Don't blame companies for convoluted Privacy Practices. Available at: [Op-ed: Don't Blame Companies for Convoluted Privacy Policies - Lexology](#) [Accessed 16/04/2022]

Crawford, Kate. (2017). The Trouble with Bias. Keynote at Neural Information Processing Systems (NIPS'17). Available at: [The Trouble with Bias, by Kate Crawford \(Revolutions\) \(revolutionanalytics.com\)](#) [Accessed 26/03/2022]

Dastin, J., 2018 "Amazon scraps secret AI recruiting tool that showed bias against women" Reuters. Available at: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G> [Accessed 24th February 2022]

Esayas, Samson, (2015). The Role of Anonymisation and Pseudonymisation Under the EU Data Privacy Rules: Beyond the 'All or Nothing' Approach European Journal of Law and Technology, Vol 6, No 2, 2015, Available at SSRN: <https://ssrn.com/abstract=2746831> [Accessed 14/04/2022]


EU GDPR, (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR). Available at: <https://www.legislation.gov.uk/eur/2016/679/contents> [Accessed 14/04/2022]

Gunn, J., Beverly-Smith, H., (2021). Significant Changes Proposed to UK GDPR. Available at: [Significant Changes Proposed to U.K. GDPR | Publications | Insights | Faegre Drinker Biddle & Reath LLP](#) [Accessed 18/04/2022]

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems*, 47, 98-115. Doi: 10.1016/j.is.2014.07.006

Hines, Caitlin. 1999. Rebaking the pie: The woman as dessert metaphor. Reinventing identities: The gendered self in discourse, ed. by M. Bucholtz, A.C. Liang & L.A. Sutton, 145-62. New York, Oxford: Oxford University Press.

House of Lords, (2018): House of Lords, Select Committee on Artificial Intelligence, AI in the UK: ready, willing and able? available at: [https://publications.parliament.uk/pa/ld201719/ldselect/ldai\\_/100/100.pdf](https://publications.parliament.uk/pa/ld201719/ldselect/ldai_/100/100.pdf) [Accessed 24th February 2022]



ICO, Information Commissioner's Office, (2018), Personal Data Breaches. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatisa> [Accessed 14/04/2022]

ICO, Information Commissioner's Office, (2020), Penalty Notice Marriott International Inc, Available at: <https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf> [Accessed 14/04/2022]

Irwin, L., (2022). What exactly is personal data? Available at: [The GDPR: What exactly is personal data? - IT Governance Blog En](#) [Accessed 18/04/2022]

Afifi-Sabet, K, (2021). UK reveals post-Brexit data reforms alongside flurry of international agreements. Available at: <https://www.itpro.co.uk/policy-legislation/general-data-protection-regulation-gdpr/360694/uk-post-brexit-data-reform> [Accessed 01/05/2022]

Keen, (2020), The ever-growing weaknesses of anonymised data: Available at: <https://hazy.com/blog/2020/04/08/weaknesses-of-anonymised-data/> [Accessed 14/04/2022]

Kilbertus, N., Rojas Carulla, M., Parascandolo, G., Hardt, M., Janzing, D. and Schölkopf, B., 2017. Avoiding discrimination through causal reasoning. *Advances in neural information processing systems*, 30.

Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. *Telecommunications Policy*, 37(4-5), 372-386.  
Doi:10.1016/j.telpol.2012.04.011

Layton, R. (2019). The 10 Problems with GDPR. Available at: [Layton Testimony1.pdf \(senate.gov\)](#) [Accessed 16/04/2022]

Leavy, S., (2018) "Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning," *2018 IEEE/ACM 1st International Workshop on Gender Equality in Software Engineering (GE)*, 2018, pp. 14-16.

Marriott, (2021), MARRIOTT GROUP GLOBAL PRIVACY STATEMENT. Available at: <https://www.marriott.com/about/privacy.mi> [Accessed 14/04/2022]

Mitchell, Tom M., et al. 1997, "Machine learning" pp. 870–877.

Nadeem, Ayesha; Abedin, Babak; and Marjanovic, Olivera, (2020) "Gender Bias in AI: A Review of Contributing Factors and Mitigating Strategies". *ACIS 2020 Proceedings*. 27. <https://aisel.aisnet.org/acis2020/27> [Accessed 24th February 2022]

NYTimes, (2021). Some Hotels are Mandating Vaccines, Will Others Follow? Available at: [Some Hotels Are Mandating Vaccines. Will Others Follow? - The New York Times \(nytimes.com\)](#) [Accessed 18/04/2022]

Parsheera, Smriti, (2018). A Gendered Perspective on Artificial Intelligence. Proceedings of ITU Kaleidoscope 2018 -- Machine Learning for a 5G Future, Available at SSRN: <https://ssrn.com/abstract=3374955> or <http://dx.doi.org/10.2139/ssrn.3374955> [Accessed 24th February 2022]



Pinsent Masons (2013). Data protection enforcement in UK, France and Germany explained. Available at: [Data protection enforcement in UK, France and Germany explained \(pinsentmasons.com\)](https://pinsentmasons.com) [Accessed 18/04/2022]

Sorensen, E., (2021). GDPR Adequacy Decision for the UK. Available at: [GDPR adequacy decision for the UK - activeMind.legal](https://www.activemind.legal) [Accessed 18/04/2022]

Statista, (2022). Revenue of Marriott International Inc Worldwide from 1999 to 2021. Available at: [Marriott revenue worldwide 2021 | Statista](https://www.statista.com/statistics/1111111/marriott-revenue-worldwide/) [Accessed 18/04/2022]

Terrell J, Kofink A, Middleton J, Rainear C, Murphy-Hill E, Parnin C, Stallings J. (2017) Gender differences and bias in open source: pull request acceptance of women versus men. *PeerJ Computer Science* 3:e111 <https://doi.org/10.7717/peerj-cs.111> [Accessed 24th February 2022]

UK, (2020), UK Data Ethics Framework. Available at: [Data Ethics Framework - GOV.UK \(www.gov.uk\)](https://www.gov.uk) [Accessed 14/04/2022]

Wang, L. (2020). The Three Harms of Gendered Technology. *Australasian Journal of Information Systems*, 24. <https://doi.org/10.3127/ajis.v24i0.2799> [Accessed 24th February 2022]

Yapo, Adrienne., Weiss, Joseph., 2018 “Ethical Implications of Bias in Machine Learning” 10.24251/HICSS.2018.668