ASSESSING THE PROTECTION OF THE GDPR ON MARGINALISED COMMUNITIES

Arnav Bawa, OP Jindal Global University

Introduction

Information is one of the most powerful tools that one could possess. This is one of the sole principles that companies use while providing its services. One of the key functions of companies that provide free services is collecting data from its customers to understand what their customers like and dislike. They then use this information to create a profile on their customer, with the data that is sold across various platforms to build upon the profile and reach a position where the companies could predict the behaviours of their customers, based on the data they have collected and the profile that they have created. For example, a who person likes a lot of super hero films, would tend to naturally search for certain superhero merchandise on the internet. Even if they enter a search for a product on Google or directly on Amazon, they might be prone to receiving ads on superhero merchandise on Facebook or Instagram. This occurs due to the sale of data that takes place behind the scenes and consumers have little to no information on such instances. One might think that this is helpful, sure who would not want personalised ads tailored to their choices? Profiling might be helpful when it comes to persons, since they receive a better customer experience and are more likely to get faster and more efficient service with the business using its predictive algorithm. The only problem is that the stakes for certain individuals might be higher, where their internet activity may be a life or death situation.[1]

Who is in a Life-or-Death Situation?

Persons who experience discrimination offline are prone to facing some sort of discrimination even online, so the digital footprint that they leave can pose a great risk.[2] Take an example of a person signing up for a queer dating app, the third parties can collect and even compile their

[1]Callum Tennent, 'The Importance of Digital Privacy for Marginalized Groups' (Web Foundation, 2021) <https://webfoundation.org/2021/10/the-importance-of-digital-privacy-for-marginalized-groups/> accessed 23 April 2023.
[2] Ibid

data to build a profile. This can later be bought or legally seized by authorities (depending on their legislation) and identify persons whose sexual identity is not made public. This was done in Egypt, the police had used the app Grindr, which is a queer dating app to track and torture persons who were part of the LGBTQ+ community and its geolocation feature within the app aided in their arrests.[3] The situation with the members of the LGBTQ+ community became so dangerous in countries which have discriminatory laws, that Tinder provided a feature where it would warn persons with an LGBTQ+ profile to be wary of using the platform in certain countries.[4] What is worse is that apps such as Grindr and OkCupid collect certain health data such as sexually transmitted diseases and share that with third parties.[5] Even publicly shared data can be used against any individual, for example, in Afghanistan, after the Taliban's takeover, people of the LGBTQ+ community have been targeted by them for their 'liberal thoughts' and contacted these individuals through social media.[6] The US also uses social media and online surveys to track down migrants and deport them, through information that they purchase from data brokers.[7] The purpose of this section in the paper, is not only to talk about who is susceptible to certain acts by authorities, but also to highlight the importance of people's digital footprint.

Some would argue that the problem lies with there being no distinction between the persons who are more vulnerable in the field of data privacy. Vulnerability is the susceptibility to certain harm, these are specifically racial minorities, asylum seekers and person with disabilities.[8] Presently, a universalistic approach is followed, wherein privacy and data protection apply to all persons equally.[9] The particularistic approach is followed in cases of children, since neither do they possess enough experience or awareness of the risks that comes

[3] Daniel Villarreal, 'Egyptian Officials Systematically Abuse, Torture Gays, Rights Group Says' (NBC News, 25 October 2020) <https://www.nbcnews.com/feature/nbc-out/egyptian-officials-systematically-abuse-torture-gays-rights-group-says-n1244755> accessed 2 May 2023.
[4] Sara Ashley O'Brien, 'Tinder Is Rolling Out A Travel Alert Feature To Protect LGBTQ Users' (CNN, 24 July 2019) https://edition.cnn.com/2019/07/24/tech/tinder-lgbtq-travel-alert/index.html accessed 26 April 2023.
[5] Natasha Singer and Aaron Krolik, 'Grindr and Other Gay Dating Apps Want to Create Connections Outside of the Bedroom' (The New York Times, 13 January 2020) https://www.nytimes.com/2020/01/13/technology/grindr-apps-dating-data-tracking.html accessed 2 May 2023.
[6] Callum Tennent, 'The Importance of Digital Privacy for Marginalized Groups' (Web Foundation, 2021) <https://webfoundation.org/2021/10/the-importance-of-digital-privacy-for-marginalized-groups/> accessed 23 April 2023.
[7] The Brennan Center for Justice, 'Social Media Surveillance in Homeland Security Investigations: A Threat to Free Speech and Privacy' (The Brennan Center for Justice, 16 November 2019) https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-homeland-security-investigations-threat accessed 2 April 2023.
[8] Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 3.
[9] Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 4.

with using the internet, nor do they understand the innate data collection driven architecture that is used. However, age should not be the only criteria for protection of data subjects. There is a difference between between the vulnerability that arises from both data processing and the outcome of such processing. Where the limitation on such knowledge on the nature of processing may be due to various other factors maybe like age, disability or the socio-economic capabilities of an individual.[10] This brings us to the examination of the European Union's General Data Protection Regulation (GDPR), which is termed to be the father of all privacy legislations, since it is one of the most strict legislations that related is to data privacy. The GDPR[11] introduces various rights that aim to be addressed form the various complexities and informative rights that are bestowed upon the data subjects.

The Transparency's Opacity

The EU GDPR under Article 12(1) mandates a communication by the data controller to the data subject on their rights in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.[12] The utmost importance that can be inferred from Articles 12, 13 and 14[13], is transparency between the data controller and the data subject. The purpose of these Articles are to ensure that data subjects are made aware by the data controllers themselves, on the rights that are available to them, the data that is collected by them and whether it may or may not be sold to a third party. Prior to the enactment of the GDPR, most people overlooked the privacy policies found within websites or apps, however, with the stricter and more comprehensive data protection law there is a mandate on such privacy policies to be provided.[14]

A comparative analysis between the privacy policies prior to the enactment of the GDPR and post the enactment of the GDPR was conducted.[15] This concluded that companies were affected in different ways, however, what remains consistent between both periods is that they are long, with an average reading time of roughly seventeen minutes and twenty seconds for an individual privacy policy.[16] The problem lies with the complexities that the GDPR introduced.

[10]Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 5.
[11] EU General Data Protection Regulation, Regulation (EU) 2016/679.
[12] General Data Protection Regulation (EU 2016) art 12(1).
[13] General Data Protection Regulation (EU 2016) art 13; General Data Protection Regulation (EU 2016) art 14.
[14]Rob Sobers, 'How Privacy Policies Have Changed Since GDPR?' (14 October 2022) Varonis Blog https://www.varonis.com/blog/gdpr-privacy-policy accessed 24 April 2023.
[15] Ibid
[16] Ibid

While it is necessary for individuals to be informed of their rights, it is unreasonable for individuals to read lengthy documents that consists of many technicals terms and legal jargon which overall requires a higher level of reading by the data subject. Companies should not only provide a transparent, concise and easily accessible privacy policy for children, but for every data subject. The purpose of privacy policies are to be informative and have a certain force of law since it does have an impact on people's rights. However, it cannot serve its purpose if each privacy policy requires a lawyer's lawyer to read it and provide their understanding for the same. Building upon the analogy of law and privacy policies, for people to be aware of the law and act in a manner where the law can guide them cannot be achieved with an exhaustive and technical privacy policy. Therefore, it is not only in the interest of the data subjects, but also in the interest of the data controller for there to be a more concise and less technical privacy policy. Data controllers would benefit since it would comply with the GDPR, a clear and transparent policy could improve the reputation of a company with its customers and stakeholders. Lastly, they companies could benefit as stronger privacy policies could provide them with an edge over their competitors.

Addressing the vulnerable data subjects, 50% of the entire population of minorities are below the poverty line in the US (there is no official body that publishes such information on the EU, hence using an inference from the US's population).[17] They face discrimination online and offline, especially with the use of personal information such as race or sexuality which may be used as a factor while being granted certain opportunities such as employment or admission to educational institutions.[18] Therefore, privacy policies should be easily legible to those at least with only a higher secondary education degree. Over 60% of the privacy policies reviewed from 150 policies from leading tech companies, found a minimum reading level of at least a college degree and over 15% are at a level of a professional career.[19] Hence, with all the legal jargon and complexities introduced by the GDPR, vulnerable data subjects would not be able to access their rights introduced by the GDPR since they cannot access the document which helps exercise their rights.

[17] American Psychological Association. (2017, July). Ethnic and Racial Minorities & Socioeconomic Status. Retrieved from https://www.apa.org/pi/ses/resources/publications/minorities.
[18] Privacy for America. (2021, May 28). How Equity and Privacy Go Hand in Hand. Retrieved from https://www.privacyforamerica.com/how-equity-and-privacy-go-hand-in-hand/
[19] Kevin Litman-Navarro, 'We Read 150 Privacy Policies: They Were an Incomprehensible Disaster' (2019) The New York Times https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html accessed 2 May 2023.

Privacy and Equity

We will need to breakdown certain provisions of the GDPR to better understand the relationship between privacy and equity. For this the GDPR's relationship with vulnerable data subjects needs to be understood. Under Recital 75 of the GDPR, there is a particular reference of vulnerable natural persons to mean only children, but at the same time acknowledges that there are risks to rights and freedoms of natural persons of varying likelihood and severity that may result from the processing of natural data.[20] It also classifies personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union memberships, and genetic data, biometric data as special categories of personal data under Article 9(1)[21], that may not be processed unless Article 9(2)[22] is complied with. Special categories or sensitive personal data does carry a higher risk to the privacy of a person. However, considering that children are specifically vulnerable, and their vulnerability is recognised by the GDPR infers that there is only a particularistic approach to vulnerability and not universal, i.e., it finds that only children are vulnerable.[23]

Consent and Privacy Policies

Under the GDPR children below the age of 16 or in some cases 13 cannot consent to the processing of their personal data, unless consent is given by the holder of parental responsibility over the child.[24] The GDPR separates personal data and sensitive personal data, which shows that certain data should be protected at a higher threshold, however, under Article 9(2)(a)[25], explicit consent is enough for such processing. It should also be noted that consent has been widely criticised for not being the adequate means through which companies may process their data.[26] As highlighted in the previous section, privacy policies are lengthy and exhaustive documents to read since it mainly consists of technical jargon which makes it difficult on the average consumer to read. Therefore, a survey found that 91% of consumers consent to legal terms of service or privacy policies without reading them, hence it can even be argued that

[20] European Union, General Data Protection Regulation (2016/679/EU), Recital 75.
[21] General Data Protection Regulation (EU 2016) art 9(1).
[22] General Data Protection Regulation (EU 2016) art 9(2).
[23] Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 6.
[24]General Data Protection Regulation (EU 2016) art 8(1).
[25] General Data Protection Regulation (EU 2016) art (9)(2)(a).
[26] Gayathri Murthy and David Medine, 'Data Protection and Financial Inclusion: Why Consent is Not Enough?' (2019) CGAP, accessed 2 May 2023, https://www.cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough.

consent in such case is not free consent, as there may be no other sufficient alternatives, thereby forcing consumers to use their service in exchange for data processing even if it may be free.[27]

As it has been established above, consumers do not read privacy policies. This leads to an examination of the bargaining position. Consumers who would like to avail a free service would normally tend to be at a worse bargaining position, than that of the companies who provide the free service. For example, take Instagram, many generations have signed up on the app to connect to one another, if an individual wished to stay off the platform the consequence would be that they would not be able to connect to their friends. This would be difficult since humans are social beings and not being able to connect or the feeling of being left out would force them to join the platform. Thereby, the bargaining position that Meta (Instagram's parent company) have versus the position of the individual is far better. Therefore, the only choice an individual is left with is to accept the terms and conditions or to not connect with their friends. Hence, people are forced not only due to a company's ambiguous and lengthy privacy policy but are to made to sacrifice on certain personal data in order to connect.

The point of the argument above is that, even if the GDPR sticks to its universalistic approach to processing of data, one way in which it could safeguard the privacy of individuals would be by requesting consent at different stages of using a service. The request for accessing certain personal data should only be requested at a stage where it would be required by the app for its actual function and not at right at the beginning with universal consent to be provided for every single function of the service. Implementing a stage wise request for consent along with a concise excerpt on the need for the accessing such data along with the data subject's rights and obligations in a clear and legible manner, such that even data subjects without a college degree would be able to follow. This would allow data subjects to have more control over the personal data that they provide and limiting the information paradox that exists between data subjects and vulnerable data subjects.

As stated previously, vulnerable subjects within the GDPR follow a particularistic approach, however, it follows a universal definition for a data subject, with a certain groups such as children being classified as a high risk group.[28] However, from the arguments above it can also be inferred that marginalised communities be vulnerable data subjects since the primary

[27] Ibid.
[28] Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 6.

argument that the GDPR makes within recital 38 is the lack of awareness of a child; and this can be the same lack of awareness that maybe present within marginalised communities. The issue of valid consent and the power imbalance between a child and data controller also similarly exists and the same has been applied to the case of vulnerable adults, where a link is established between the power imbalance and vulnerability of data subjects.[29]

Automated Decision-Making and Vulnerable Data Subjects

Recital 75 reasons that vulnerable data subjects are categorised separately due to the impact that it may have on the rights and freedoms as a result of personal data processing. Taking an example of Artificial Intelligence (AI) bias, or bias within automated data processing, since human biases are within the data used for training an AI or building an algorithm, some data subjects maybe more prone to discrimination from processing data as a result. The problem lies with the biased data used to train and the opaque yet actionable decisions provided by automated machines. Article 22 ensures that data subjects shall have a right to not be subjected to a decision that is made solely on automated processing.[30] However, the same right is restricted under Article 23 for the purpose of national security, defence, public security, etc. as mentioned under Article 23.[31] Member States of the EU can argue the need for using algorithmic governance tools for their borders in deciding whether or not to grant asylum to asylum seekers since they can argue that it is in the interest of national security or any one of those above mentioned restrictions. Ireland uses facial recognition and algorithms to grant welfare benefits to its citizens, but it has been criticised by the Irish Council for Civil Liberties for collecting more personal data than necessary for confirming identity of individuals.[32] This directly relates to persons with lesser economic capabilities are required to surrender more personal data than would be necessary by another data subject. Showing how privacy may be available to only those who can pay for it. Another example of the same, is with ChatGPT's (OpenAI's text based generative chatbot) update to their terms of service. The GDPR mandates a data protection by default policy under Article 25[33], under ChatGPT's recent update to its privacy policy the data protection by default setting was only for those who used a premium

[29] Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 6.
[30] General Data Protection Regulation (EU 2016) art 22.
[31] General Data Protection Regulation (EU 2016) art 23.
[32]Human Rights Watch, 'How EU's Flawed Artificial Intelligence Regulation Endangers Social Safety Net' (10 November 2021) https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net.
[33] General Data Protection Regulation (EU 2016) art 25.

account and not for those using a free account. The distinction between the two is that, by default, the AI chatbot would not collect the data and chats between the users and AI for the premium subscribers, while it would collect it by default for the free users. France's Caisse does Allocations Familiale (CAF), a government agency that uses an automated system to calculate and distribute social security benefits.

The above mentioned examples provides how despite a restriction being placed on data subjects being subjected to automated decision making, the exceptions to the same are broad and generally can apply to persons with a higher risk due to processing. This also raises several alarms on privacy being available to those who can pay for it rather than a universal right since individuals to make avail of certain benefits surrender more personal data than those who do not.

Recognising Vulnerable Individuals

Vulnerable data subjects as found in the GDPR is built on the idea of unequal power dynamics and lack of awareness which applies in the case of children. Prior to the GDPR's enactment, there have been several instances where courts have tried to highlight the individuals who fall within the ambit of being vulnerable to harm. The case of Dudgeons v. UK, found that where the moral interests and the welfare of individuals who were in need of special protection due to a lack of maturity, mental disability or a state of dependence. This shows how vulnerability is founded on weakness, inexperience and dependence[34], thereby, it can be argued that the dependence of those relying on State aid can be classified as vulnerable. The GDPR should inculcate such tacit recognition of the individuals who face discrimination as vulnerable and create higher thresholds for protecting such individuals' data.

The Council decision on the European Social Fund found that there are categories of persons who are particularly vulnerable on the labour market; such as women, persons with disabilities and migrants.[35] Such individuals who face discrimination in one legal sector may make them more susceptible to facing discrimination in other sectors therefore, it becomes necessary to mitigate opportunities of their discrimination.

[34] Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 8.
[35] Malgieri, G. and Niklas, J., 'Vulnerable Data Subjects' (2020) 6 Computer Law & Security Review 9.

Recommendations

Firstly, through this paper it has been highlighted multiple times to recognise that the personal data of individuals from marginalised communities is susceptible to more harm hence, it requires a general recognition with a similar threshold for the protection of children's personal data. Secondly, social media entities should be platforms that allow people to explore their identity, so it should be a safety net and not a tool that could be used against them. Lastly, the burden of responsibility at the end lies with the data subject. For them to make informed decisions, they need to receive clear and concise information through privacy policies since the informational paradox is one that creates confusion. Consent can only be freely given when there is complete information symmetry and a clear demarcation of what personal data is collected and the reason for its collection and processing; with also an alternative remedy than it being *"my way or the highway"* as companies do no permit use of their services unless consumers consent to their privacy policies.

Conclusion

The use and collection of personal data by State authorities and companies have a significant threat to individuals, specifically those individuals who face discrimination offline and not only online. The purpose for profiling for such companies is to offer personalised services and advertisements, however, the risk of misuse of data of vulnerable data subjects and its probability of abuse should be something that the GDPR considers. This raises the need for short and concise privacy policies, that are able to be transparent and legible to the general public, without college or professional degrees.

The regular examination of privacy laws is something that is paramount due to technological advancements. A continuing discussion wherein the implications of such laws is considered would ensure that the vulnerable data subjects' rights are upheld. Heavy emphasis is laid on this point is due to the potential damage that may be caused to them as a result of misusing their data. Hence, companies and authorities should take responsibility to ensure that data subjects are aware of their rights and the reasons for which their data is being processed. Privacy is a natural human right[36], which should be available to all and not only to those who can pay for it.

[36] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.