"Passed by the European Union in 2016, the General Data Protection Regulation (GDPR) came into effect on May 25th of 2018 as an all-encompassing privacy law aimed at regulating how corporations collect, store and utilize EU citizens' personal information strictly. It aims at ensuring safety regarding individuals' privacy while promoting supervision towards corporate conduct involving collected data belonging to them across multiple locations. This is regardless of its scale globally. Amongst many critical elements present within this legislation include clauses such as being forgotten because everyone deserves a clean slate from past errors without being haunted by prior actions or comments that might affect them later; Receiving authorization for access towards your own self-shielded private details serves intelligence in providing control toward protective measures implemented in daily life with regard globally against internet predators too; demanding appropriate portability concerning your defined data part can serve as a preferable alternative, avoiding unnecessary steps or issues for both parties involved instead of re-entering identical personal information every single time; Lastly, providing prompt notifications regarding possible data breaches at stake via the likes of official communication channels may serve well in avoiding casualties from certain instances purely caused because lack of awareness regarding negligent practices. Businesses must comply with these regulations to avoid substantial cash fines amounting up to €20 million or 4% of global revenue. Thus, GDPR's implementation could revolutionize how companies handle personal information and raise individuals' awareness of privacy rights. Not all companies can comply with data management regulations, and small businesses often struggle the most due to insufficient resources causing slow implementation of necessary changes. According to our analysis based on Kantian ethics, adopting tough measures on data privacy is crucial for America. Keeping to Kantian ethics, GDPR respects people's privacy rights by giving them control over their data. Upholding this regulation ensures that individuals' interests are prioritized by considering them not as tools but as ends in themselves.

135 words and needs more on GDPR(fixed)

Zimmer's (2010) article "But the data is already public": On the ethics of research in Facebook," a discussion on data ownership is presented in relation to the ethical implications of conducting research on Facebook. Through comparing Facebook users' assumption of owning their data and contradicting policy terms, there exists a tension illuminated in the article.Accordingly stipulated in the article titled "GDPR: An executive guide as regards essential terms one should know" published by ZDNet, individuals enjoys being vested upon by the framework defined within GDPR when it comes to ownership rights pertaining to digital assets. Moreover, business entities playing major roles in this arena must adhere and seek permission directly among those who want consented involvement prior utilization of it.The significance awarded to individuals' control over their personal information can be observed when reviewing the ZDNet article through a data ownership lens, revealing how GDPR safeguards these privileges. Organizations handling such information must demonstrate respect for individuals' proprietary claims towards their personal records, which includes obliging with explicit consent procedures as well as ensuring transparent and legal handling. The concept of data ownership, as discussed in Zimmer's article and applied to GDPR, highlights the importance of respecting individuals' rights over their personal data. This includes ensuring that individuals have control over their personal data, and organizations and researchers obtain explicit consent before processing or using it. GDPR provides a legal framework to protect these rights and promote ethical data practices. According to Zimmer, a key concept of Kantian ethics is the principle of respect for persons, one of the cornerstones of the author's article. As a consequence of this principle, the individual is required to be viewed as an end in itself rather than as merely a means to some other end. It's Zimmer's contention that the collection and analysis of Facebook user data without the consent of the users breaches this principle, thereby endangering the privacy of those users. I find Palmer's case on the ZDNet article to be an important reminder that "the right to privacy extends to the rights of individuals.". Among the many things GDPR seeks to protect is the citizens' right to privacy, as well as provide them with a greater sense of agency when it comes to their own data. A regulation implementing this legislation establishes a clear consent process in which companies must obtain and process the user's consent before they can obtain and process their personal information. It is nevertheless true that a number of entities are struggling with regulatory compliance issues in light of the huge monetary sanctions mentioned here, resulting in hefty fines. The Kantian analysis reveals that following only formal regulations without considering the principles contained within them would be a highly inadequate approach to morality. To fulfill their moral responsibilities to their users, companies must respect the privacy rights of those users and ensure that they obtain informed consent from them before gathering or processing any sensitive information about them. As a result of these commitments, we are abiding by the fundamental notion of

respecting individual rights, whereby individuals are treated as rational creatures capable of making their own decisions without external interference. As such, it's beyond doubt that organizations must honor these duties towards their clients irrespective of any regulatory specifications like GDPR compliance which in itself may not entirely guarantee compliance with these obligations. Ethically speaking, companies must prioritize the protection of individual privacy by adopting proactive measures designed to secure individual consent prior to collecting or processing any personal data. Business should, therefore, invest in robust data privacy policies and procedures, as well as a user-friendly website, as a way to give users a full understanding of how their information will be utilized, no matter what the costs may be. Section is 385 words. Zimmer needs further articulation and more role in analysis (fixed)

With a case study on analyzing Twitter activity related to ISIS/ISIL, Buchanan(2017) investigates the moral complexities associated with big data research techniques. Data mining and machine learning algorithms are both essential components of this type of investigation. This study raises concerns about privacy and ethical considerations associated with deploying such technologies on mammoth datasets obtained through social media networks. Monitoring individuals' right to safeguard confidential information while controlling collected personal information processing is made possible through regulatory requirements stipulated in GDPR (General Data Protection Regulation) enforced by EU member states. Taking into account big-data-computing approaches like empirical analyses alluded to in "GDPR: Everything you need to know about the new general data protection regulations," raises concerns on accumulating personal information without permission potentially resulting in breaches of private entities concerns.Big Data research poses certain ethical quandaries concerning privacy breaches. GDPR mandates that organizations obtain explicit consent from individuals before processing their personal information while ensuring lawful and fair treatment. To conduct Big Data research ethically, informed consent coupled with risk assessment is particularly important in willful compliance with the law, according to Buchanan's article. The ethical repercussions associated with gathering large-scale individualized datasets show how challenging the introduction of the GDPR is—the legislation calls for appropriate safeguards when concerning fundamental aspects such as individuals' rights to their privacy or lawfully processing their information. Because this directly impacts big-data research, complying with such regulation becomes essential within responsible usage practices. A significant dilemma posed by big data research involves the possibility of bias and prejudice towards specific groups emanating from these

practices. Machine learning algorithms extensively utilized within these procedures are prone to incorporating biased ideas stemming from inadequate datasets hence reinforcing current stereotypes or social inequities underlining various communities' lives. Thus, it necessitates ethical guidance coupled with stringent supervision in overseeing both the creation processes and implementation phases of these systems assuring users have an equitable advantage. Big data research poses serious ethical dilemmas, especially pertaining to the perilous outcomes that may arise for both individuals and different social collectives involved. The imperative nature of focusing on marginalized persons or communities has been emphasized by Buchanan's article as a crucial criterion of ethical investigation practices. To achieve this goal whilst reducing negative consequences from this research activity altogether requires due consideration for such issues as risk assessments involving informed consent procedures at all stages along the way. Big Data Research carries pressing ethical questions concerning the collation, examination, and application of personal information. In this respect, GDPR lays out legal regulations for upholding individuals' privacy rights in alignment with ethics on handling sensitive information when conducting Big Data research. Conducting ethical deliberations such as procuring informed consent with perceptions on risk assessment and avoiding discrimination are fundamental in effecting the responsible exercise of Big Data.. a fundamental principle of Kantian ethics, is pertinent in the use of big data analytics to examine social media interactions pertaining to terrorist groups such as ISIS/ISIL. Researchers must ensure that they treat individuals featured in the dataset with dignity and not solely exploit their data as a means to an end. To this end, researchers are responsible for obtaining informed consent from individual Twitter users whose tweets are included in the study while ensuring that no harm befalls them or any community. Discrimination and profiling are unacceptable practices during research activities. Researchers should avoid utilizing data pertaining to an individual's national origin, race or religious beliefs. Upholding a commitment to respecting individuals' rights can help ensure that research ethics are upheld throughout the duration of any study. In the case of GDPR, it is evident that the EU's decision to implement strict regulations on data privacy and protection is in line with Kantian principles. By prioritizing the protection of individuals' personal data, GDPR emphasizes the inherent value and autonomy of each individual. Additionally, the regulation aims to prevent individuals' exploitation for commercial or political purposes. Section is 363 words. Relation to GDPR need further development (went more into detail with gdpr)

Similarly, in Zimmer's analysis of Facebook's controversial emotional contagion study, the use of users' personal data without explicit consent is a clear violation of Kantian principles. The study aimed to manipulate users' emotions for scientific research, without taking into account each individual's autonomy and dignity. By treating users as a means to an end, rather than as ends in themselves, Facebook failed to respect their autonomy and dignity. Finally, Buchanan's case study on Twitter's use of big data to research ISIS/ISIL provides a more complex analysis. While the research aimed to better understand and prevent terrorist activity, the use of Twitter users' personal data without explicit consent or transparency raises concerns about Kantian principles violation. However, the study's ultimate goal of protecting individuals and preventing harm to society could be seen as aligned with Kantian principles. This is if it is viewed as treating each individual as an end in itself and protecting their autonomy and dignity. In conclusion, the use of personal data for research purposes requires a balance between the benefits of the research and the ethical principles of respecting individuals' autonomy and dignity. While research benefits can be significant, researchers must prioritize the protection of individuals' personal data and respect their autonomy and dignity. By using Kantianism as a guiding principle, researchers can ensure that their research is conducted ethically and in line with fundamental principles of respect for human beings. works