Kesner Pierre

BUS428

Professor: Suzanne Hartl

July 2, 2023

Term paper

“Ethical Implications of Data Privacy in the Digital Age”

In today’s interconnected world, where personal information is increasingly collected, stored, and analyzed by organizations, the ethical implications of data privacy have become a pressing concern. This essay aims to explore the ethical issue of data privacy and its implications, analyzing various perspectives on the subject. Drawing from personal experiences and an examination of different viewpoints. I will reflect on the lessons this issue has taught me about myself, ethics, and some other research to state why I hold the views I do.

To refer to the term data privacy and its challenges, we would like to highlight first the meaning of data privacy as we understand it refers to the protection of an individual’s personal information, ensuring that it is collected, stored, and used in a manner that respects their rights and autonomy. However, advancements in technology and the rapid growth of data-driven industries have presented significant challenges to maintaining data privacy. These challenges include the collection of vast amounts of personal data, data breaches, algorithmic bias, and the potential for unauthorized surveillance, etc.

The collection of personal data has become pervasive in various aspects of modern life, from online interactions to consumer behavior tracking. While data collection can have benefits, such as improving services or personalizing experiences, it raises ethical concerns related to privacy, consent, and potential harm. Therefore, the ethical issue lies in finding a balance between the benefits that can be derived from data collection and the potential risks to individual privacy and autonomy. This balance requires robust ethical frameworks, legal protections, and responsible practices by organizations to ensure that personal data is treated with integrity, transparency, and respect for individuals' rights.

One perspective we notice, as mentioned earlier, is the utilitarian viewpoint that justifies data collection based on the overall societal benefits it may bring. However, critics argue that this perspective often overlooks or undervalues the potential negative consequences, such as breaches of privacy, data leaks, or the misuse of personal information for surveillance or discrimination.

From a rights-based perspective, individuals have a fundamental right to control their personal information. This perspective emphasizes the need for informed consent, transparency, and the ability to make decisions regarding data collection and usage. Critics of extensive data collection argue that it infringes upon individual autonomy and privacy rights, potentially leading to abuses and violations of personal boundaries. As a result of the collection of vast amounts of personal data, research shows that "numerous government agencies, including the FBI, Department of Defense, National Security Agency, Treasury Department, Defense Intelligence Agency, Navy, and Coast Guard, have purchased vast amounts of U.S. citizens' personal information from commercial data brokers. The revelation was published in a partially declassified, internal Office of the Director of National Intelligence report released on June 9, 2023".

"https://www.route-fifty.com/tech-data/2023/06/us-agencies-buy-vast-quantities-personal-information-open-market/38"

The report shows the breathtaking scale and invasive nature of the consumer data market and how that market directly enables wholesale surveillance of people. The data includes not only where one has been and who one is connected to, but the nature of one's beliefs and predictions about what one might do in the future. The report underscores as well the grave risks the purchase of this data poses and urges the intelligence community to adopt internal guidelines to address these problems.

To defend itself in this situation, the government highlights different approaches in order to justify its involvement in purchasing the vast amount of U.S. citizens' information from commercial data brokers. Such as national security and crime prevention perspective,

proponents of this perspective argue that government agencies' access to vast amounts of personal information can be justified in the interest of national security and crime prevention. They contend that using data analysis and surveillance techniques can aid in identifying potential threats and preventing criminal activities. Advocates argued in the government's favor that these measures are necessary to safeguard the public and uphold the government's duty to protect its citizens.

Although some critics that government agencies' purchase of personal information emphasizes the potential infringement on individuals' privacy rights and civil liberties. They argue that the mass collection and analysis of personal data can lead to unwarranted surveillance, profiling, and breaches of confidentiality. Concerns may be raised about the lack of transparency, informed consent, and oversight regarding how this data is acquired, stored, and used.

From this viewpoint, the ethical issue lies in the lack of transparency and accountability surrounding the government agencies' actions. Advocates emphasize the importance of clear legal frameworks and safeguards to regulate the acquisition and use of personal data by government entities. Therefore, they call for stronger oversight mechanisms, independent audits, and increased transparency to ensure that citizens' rights are protected and that the collection and use of personal information align with ethical standards.

One another issue that people have to deal with when it comes to the ethical implications of data privacy in the digital age, is the data breach, as it refers to an incident where unauthorized individuals gain access to sensitive or confidential data held by an organization. We think it is a significant ethical issue as it can lead to various negative consequences for individuals and organizations alike.

From this viewpoint, data breaches are seen as a severe violation of individuals' privacy and can cause significant harm to personal information, such as financial data, social security numbers, or medical records, which can be exposed, leading to identity theft, financial loss, reputational damage, or emotional distress. Advocates argue that organizations have a moral duty to protect the data they collect from such breaches through robust security measures and encryption.

For instance, according to this perspective, organizations have a moral and legal responsibility to safeguard the personal data they collect. They should invest in robust cybersecurity measures, implement effective data protection protocols, and ensure the proper training of employees to prevent data breaches. When a breach occurs, organizations are expected to take prompt action, notify affected individuals, and provide assistance and compensation if necessary. Ethical lapses, such as negligence or failure to disclose breaches, can result in loss of trust and reputation damage.

It denotes the implication of hackers, some individuals may hold the viewpoint that data breaches are a form of activism or whistleblowing, exposing the weaknesses and vulnerabilities of organizations. Supporters argue that such breaches can serve as a wake-up call, forcing organizations to improve their security measures and accountability. However, critics of this perspective emphasize that unauthorized access to data is still illegal and can cause harm to individuals, making it an ethically dubious means of achieving change.

Personally, the issue of data breaches has taught me several valuable lessons. Firstly, it has highlighted the importance of data security and the need for organizations to prioritize the protection of individuals' personal information. As technology advances and cyber threats evolve, organizations must continually update their security measures to stay ahead of potential breaches.

Secondly, data breaches have underscored the vulnerability of individuals in the digital age. It has made me more conscious of my own digital footprint and the importance of being proactive in protecting my personal information. Practicing good cybersecurity habits, such as using strong passwords, being cautious with sharing personal information online, and regularly monitoring my accounts for suspicious activity, can mitigate potential risks. In fact, according to research by Washington Post, they found that "Heartland Data breach may well have been one of the biggest security breaches ever perpetrated.

Heartland Payment Systems, Inc. (HPS) provides debit, prepaid, and credit card processing, online payments, check processing, payroll services as well as business solutions for small to mid-sized industries. Approximately, 40% of its clients are restaurants. HPS is the fifth largest credit card processor in the United States and the 9th largest in the world.

The breach occurred in 2008 at the Princeton, N.J., payment processor Heartland Payment Systems and may well have compromised "tens of millions of credits and debit card transactions" (rebs; online). Revelations were announced to the public on January 20, 2009, the day of Obama's inauguration.

Heartland processed payments at the time for more than 250,000 businesses when it began receiving fraudulent reports from MasterCard and Visa from cards that had been used by merchants who had relied on Heartland when processing payment".

https://www.paperdue.com/topic/data-breach-essays

We have found out that the implications of the Heartland data breach were significant for both individuals and businesses. For individuals, the breach exposed their sensitive payment card information, increasing the risk of identity theft, fraudulent charges, and financial losses. Businesses that relied on Heartland for payment processing also faced reputational damage and potential legal liabilities for the security lapse.

The magnitude of the Heartland data breach underscored the importance of robust security measures and ethical responsibilities in handling sensitive customer data. It prompted increased scrutiny and awareness of the need for stringent data protection protocols within the payment processing industry and other sectors that handle personal information.

The breach also served as a catalyst for improvements in security practices, regulations, and industry standards. It highlighted the necessity for organizations to prioritize data security, implement encryption and tokenization techniques, conduct regular security audits, and promptly detect and respond to potential breaches.

The issue of ethical implications of data privacy in the digital age has raised another concern which is the concept of “algorithmic bias”, it is referred to the unjust or discriminatory outcomes that can result in decision-making processes. These concepts, (algorithms) are sets of rules or procedures followed by computers to solve problems or make predictions. Algorithms are increasingly being employed in various domains, including hiring practices, loan approvals, criminal justice, and recommendation systems. There are different factors that should be emphasized when we are talking about algorithmic bias, for instance, first from an unintentional bias perspective, the unintentional bias perspective acknowledges that algorithmic bias is often a result of the inherent biases present in the data used to train algorithms. This viewpoint argues that algorithms are neutral tools and that any biases present are a reflection of societal biases embedded in the data. The following points highlight the key elements of this perspective which is biased data, algorithms rely on historical data to learn patterns and make predictions. If the historical data is biased or reflects discriminatory practices, the algorithm may unintentionally perpetuate those biases. For example, if a hiring algorithm is trained on data that is biased against certain demographics, it may lead to discriminatory hiring decisions.

Societal reflection, proponents of this perspective argue that algorithmic bias is a reflection of broader societal biases and injustices. They contend that the biases observed in algorithms are not inherent flaws of the algorithms themselves but rather a symptom of the biases present in the data they learn from. Therefore, addressing algorithmic bias requires addressing the underlying societal biases that influence the data.

Data quality improvement: To mitigate unintentional bias, advocates of this perspective emphasize the importance of improving the quality of the data used to train algorithms. This involves identifying and addressing biases in the data, removing or minimizing discriminatory patterns, and ensuring that the data is representative of diverse populations.

Diversity in algorithm development, and promoting diversity in the development of algorithms is seen as a crucial step in mitigating unintentional bias. By including individuals from diverse backgrounds and perspectives in the development process, a wider range of biases and potential issues can be identified and addressed.

Rigorous testing and evaluation, to ensure that algorithms do not perpetuate biases, rigorous testing and evaluation procedures are necessary. This involves assessing the algorithm's performance across different demographic groups and monitoring for potential biases. Regular evaluation and fine-tuning of algorithms can help identify and rectify unintended biases.

Second, from a systemic discriminatory perspective, the systemic discrimination perspective highlights the concern that algorithmic bias can worsen existing societal inequalities and contribute to the perpetuation of systemic discrimination. Such as some critics argue that algorithmic bias can disproportionately affect marginalized communities. Due to historical injustices and social disparities, certain groups may already face discrimination and disadvantages. If algorithms perpetuate or amplify these biases, it can further entrench inequality and hinder efforts to address systemic discrimination.

Moreover, biases in algorithms can lead to unfair treatment of individuals or groups, for instance, biased algorithms used in hiring processes may disadvantage certain demographic groups, preventing them from accessing employment opportunities. This can reinforce existing disparities and limit social mobility. It may also have an historical injustice to individuals, because algorithms trained on biased data may perpetuate historical injustices. If the data used to train algorithms reflects discriminatory practices or systemic biases, the resulting algorithms may learn and replicate these biases, continuing the cycle of discrimination and marginalization.

As a matter of fact, one research detected the implication of Amazon in “algorithmic bias” in terms of employee hiring. “SAN FRANCISCO (Reuters) - Amazon.com Inc's AMZN.O machine-learning specialists uncovered a big problem: their new recruiting engine did not like women.

The team had been building computer programs since 2014 to review job applicants’ resumes with the aim of mechanizing the search for top talent, five people familiar with the effort told Reuters.

Automation has been key to Amazon’s e-commerce dominance, be it inside warehouses or driving pricing decisions. The company’s experimental hiring tool used artificial intelligence to give job candidates scores ranging from one to five stars - much like shopper’s rate products on Amazon, some of the people said.

“Everyone wanted this holy grail,” one of the people said. “They literally wanted it to be an engine where I’m going to give you 100 resumes, it will spit out the top five, and we’ll hire those.”

But by 2015, the company realized its new system was not rating candidates for software developer jobs and other technical posts in a gender-neutral way.

That is because Amazon’s computer models were trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period. Most came from men, a reflection of male dominance across the tech industry.

In effect, Amazon’s system taught itself that male candidates were preferable. It penalized resumes that included the word “women’s,” as in “women’s chess club captain.” And it downgraded graduates of two all-women's colleges, according to people familiar with the matter. They did not specify the names of the schools.

Amazon edited the programs to make them neutral to these particular terms. But that was no guarantee that the machines would not devise other ways of sorting candidates that could prove discriminatory, the people said.

The Seattle company ultimately disbanded the team by the start of last year because executives lost hope for the project, according to the people, who spoke on condition of anonymity. Amazon's recruiters looked at the recommendations generated by the tool when searching for new hires, but never relied solely on those rankings, they said".

"https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G".

Based on my ethical understanding of the Amazon case, I think the Amazon recruiting engine case indeed exemplifies the ethical challenges associated with algorithmic bias in the hiring process. It serves as a stark reminder of the potential consequences of biased algorithms and the importance of addressing these challenges. Responsible development, transparency, ongoing evaluation, and mitigation of bias are indeed crucial to promote fairness, diversity, and inclusion in hiring practices. By acknowledging and actively working to minimize algorithmic bias, I think organizations can strive for more equitable and unbiased decision-making processes in recruitment and beyond.

One another major point I have highlighted on the subject of ethical implications of data privacy in the digital age is the potential for "unauthorized surveillance". Which refers to the act of secretly monitoring or recording individuals or their activities without their knowledge or consent. As a consequence, unauthorized surveillance can pose a significant threat to privacy and civil liberties. In today’s digital age, advancements in technology have increased the potential for unauthorized surveillance. For example, to name a few of them, hacking and malware, malicious individuals can exploit security vulnerabilities in computers, smartphones, or other internet-connected devices to gain unauthorized access. This could enable them to activate cameras or microphones remotely, effectively turning these devices into surveillance tools.

Spyware and surveillance software, with the advancement of technology, there are commercially available spyware and surveillance software applications that can be installed on devices without the user’s consent. These programs can secretly monitor activities, such as keystrokes, browsing history, or even capturing audio and video.

IoT devices, the proliferation of the Internet of Things (IoT) devices, such as smart home devices, wearables, or security cameras, has increased the potential for unauthorized surveillance. If these devices are compromised, they can be used to monitor individuals or gather sensitive information.

Moreover, social media and online tracking, it’s been proven that online platforms, and social media networks collect vast amounts of user data, which can be used for targeted advertising or potentially accessed by unauthorized parties. This data can provide insights into an individual’s activities, preferences, and even their location. Therefore, I think unauthorized surveillance remains a crucial issue that needs to be taken and addressed seriously. In order to protect themselves against unauthorized surveillance, individuals can take several measures that are available to them to do so, such as keeping software up to date, by regularly updating operating systems, applications, and firmware on devices to ensure they have the latest security patches.

Or by using strong unique passwords, complex passwords, or passphrases and enabling two-factor authentication (2FA) whenever possible.

Individuals can protect themselves as well by being cautious with downloads and email attachments, because downloading files or opening email attachments from untrusted sources may contain malware or spyware.

Individuals can protect themselves as well by reviewing app permissions because they should be mindful of the permissions requested by apps before granting access to features like camera, microphone, or location data.

Or cover, and disconnect cameras and microphones, because if one has concerns about unauthorized surveillance, one should consider physically covering the cameras or disconnecting the microphones on devices when not in use.

Or by regularly checking for unusual activities, like Keeping an eye out for signs of unauthorized surveillance, such as unexpected battery drain, unusual data usage, or unexplained background noise during phone calls.

As a result of unauthorized surveillance, research shows: “News reports in December 2005 first revealed that the National Security Agency (NSA) has been intercepting Americans’ phone calls and Internet communications. Those news reports, combined with a USA Today story in May 2006 and the statements of several members of Congress, revealed that the NSA is also receiving wholesale copies of America's telephone and other communications records. All of these surveillance activities are in violation of the privacy safeguards established by Congress and the US Constitution.

In early 2006, EFF obtained whistleblower evidence (.pdf) from former AT&T technician Mark Klein showing that AT&T is cooperating with the illegal surveillance. The undisputed documents show that AT&T installed a fiberoptic splitter at its facility at 611 Folsom Street in San Francisco that makes copies of all email's web browsing and other Internet traffic to and from AT&T customers and provides those copies to the NSA. This copying includes both domestic and international Internet activities of AT&T customers. As one expert observed, "This isn't a wiretap, it's a country tap."

Secret government documents, published by the media in 2013, confirm the NSA obtains full copies of everything that is carried along major domestic fiber optic cable networks. In June 2013, the media, led by the Guardian and Washington Post started publishing a series of articles, along with full government documents, that have confirmed much of what was reported in 2005 and 2006 and then some. The reports showed-and the government later admitted that the government is mass collecting phone metadata of all US customers under the guise of the Patriot Act. Moreover, the media reports confirm that the government is collecting and analyzing the content of communications of foreigners talking to persons inside the United States, as well as collecting much more, without a probable cause warrant. Finally, the media reports confirm the "upstream" collection off of the fiberoptic cables that Mr. Klein first revealed in 2006".

"https://www.eff.org/nsa-spying"

In order to bring a reasonable solution to this situation, I think addressing the ethical implications of data privacy requires a multi-stakeholder approach involving individuals, organizations, policymakers, and technology developers. Moreover, striking a balance between the benefits of data-driven technologies and protecting privacy rights is crucial for creating a digital landscape that respects individual autonomy, fosters trust, and upholds ethical standards. We said this because we think, by working collaboratively, these stakeholders can contribute to a digital landscape that respects individual autonomy, encourages innovation, and safeguards privacy rights.

Work cited

“https://www.route-fifty.com/tech-data/2023/06/us-agencies-buy-vast-quantities-personal-information-open-market/38”.

“https://www.paperdue.com/topic/data-breach-essays”.

“https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G”.

“https://www.eff.org/nsa-spying”.