ETHICAL ISSUES IN BIG DATA

- SHIKHAR SETH
- SHUBHAM SABOO
- ANMOL DUREHA

Technology Analysis:

AI/Machine learning addresses the question of how to build computers that improves with time automatically through experience which is called experimental learning. It is one of today's most rapidly growing technical fields, lying at the intersection of computer science and statistics, cognitive science and at the core of artificial intelligence and data science. Recent progress in machine learning has been driven both by the of new learning algorithms and theory and by the ongoing explosion in the availability of online data and low-cost computation. The adoption of data-intensive machine-learning methods can be found throughout science, technology and commerce, leading to more evidence-based decision-making across many walks of life, including health care, manufacturing, education, financial modeling, policing, and marketing.

Data has become a great asset for many organizations, promising improved operations and new business opportunities. However, big data has increased access to sensitive information that when processed can directly jeopardize the privacy of individuals and violate data protection laws. Data privacy is responsibly collecting, using and storing data about people, in line with the expectations of those people, your customers, regulations and laws. It is intimately linked to autonomy and human dignity, and the principle that everyone should be valued and respected. Data ethics is doing the right thing with data, considering the human impact from all sides, and making decisions based on your brand values.

As technology becomes an increasingly important part of people's lives, data ethics must be translated into sound business practices to ensure that both internal and external interests are balanced. This begins with considering the human impact from all sides of data use, the impacts on people and society, and considering whether those impacts are beneficial, neutral, or potentially risky.

A quarter century ago, there was a generational shift in the consensus on how to respect privacy due to an emergence of personal computing, networked computing and large structured databases. That shift led to the implementation of modernized rules governing the protection of personal data. Today, we are experiencing a new generational shift, driven by the globalization of the economy and profound alterations in the digital, physical, and biological spheres we live in, creating an ever-expanding data-first interconnected digital world.

To keep up with the evolving digital world, the evolution of sustainable data ethics codes must go beyond check-the-box compliance and enforcement of the rules. New data ethics codes must objectively consider the effects of new technology and data uses beyond common understanding has on people.

Data Privacy Protection

Indeed, protecting data privacy is urgent and complex. This protection is necessary because of the ubiquity of the technology-driven and information-intensive environment. Technology-driven and information-intensive business operations are typical in contemporary corporations. The benefits of this trend are that, among other things, the marketplace is more transparent, consumers are better informed and trade practices are more fair. The downsides include socio-techno risk, which originates with technology and human users (e.g., identity theft, information warfare, phishing scams,

cyberterrorism, extortion), and the creation of more opportunities for organized and sophisticated cybercriminals to exploit. This risk results in information protection being propelled to the top of the corporate management agenda.

The need for data privacy protection is also urgent due to multidirectional demand. Information protection becomes an essential information security function to help develop and implement strategies to ensure that data privacy policies, standards, guidelines and processes are appropriately enhanced, communicated and complied with, and effective mitigation measures are implemented. The policies or standards need to be technically efficient, economically/financially sound, legally justifiable, ethically consistent and socially acceptable since many of the problems commonly found after implementation and contract signing are of a technical and ethical nature, and information security decisions become more complex and difficult.

Data privacy protection is complex due to socio-techno risk, a new security concern. This risk occurs with the abuse of technology that is used to store and process data. For example, taking a company universal serial bus (USB) device home for personal convenience runs the risk of breaching a company regulation that no company property shall leave company premises without permission. That risk becomes a data risk if the USB contains confidential corporate data (e.g., data about the marketing strategy, personnel performance records) or employee data (e.g., employee addresses, dates of birth). The risk of taking the USB also includes theft or loss.

Using technology in a manner that is not consistent with ethical principles creates ethical risk, another new type of risk. In the previous example, not every staff member would take the company USB home, and those who decide to exploit the risk of taking the USB may do so based on their own sense of morality and understanding of ethical principles. The ethical risk (in addition to technical risk and financial risk) arises when considering the potential breach of corporate and personal confidentiality. This risk is related partly to technology (the USB) and partly to people (both the perpetrator and the victims) and is, therefore, a risk of a technological-cum-social nature—a socio-techno risk. Hence, taking home a USB is a vulnerability that may lead to a violation of data privacy.

However, the problem of data privacy is not unsolvable. The composite approach alluded to earlier that takes into consideration the tangible physical and financial conditions and intangible measures against logical loopholes, ethical violations, and social desirability is feasible, and the method suggested in this write-up can accomplish this objective.

Stakeholder Analysis:

We structure our findings in terms of the three interrelated stakeholder groups: individuals, organizations, and society. The figure below summarizes the concepts by stakeholder groups and relative importance. We then elaborate on each concept in detail and explain how they give rise to ethical issues in big data analytics.

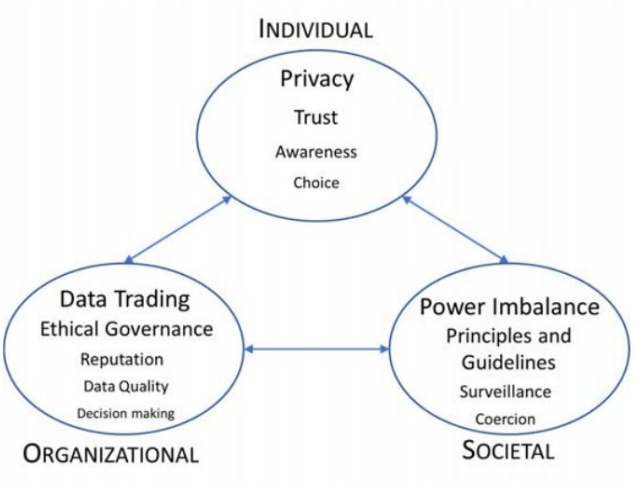
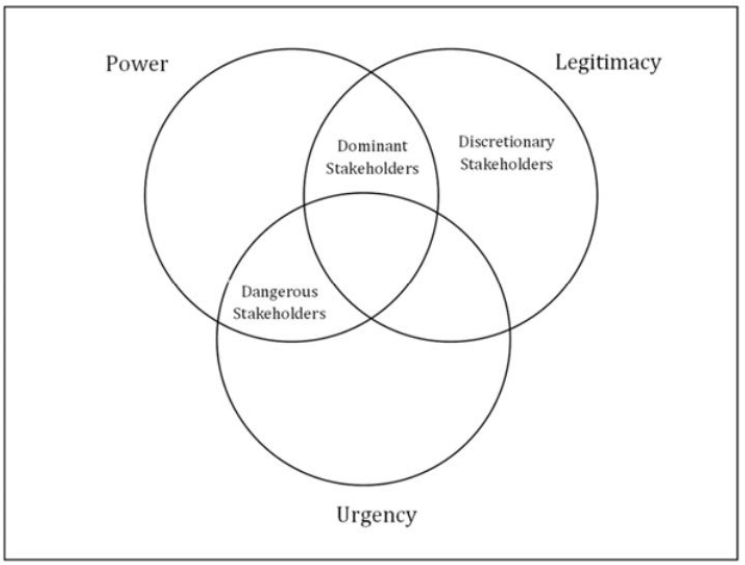


Figure 1. Concepts and Their Relative Importance to Stakeholders[2]

Three stakeholder attributes relevant to salience include their power to influence data and data management, the legitimacy of their relationship to

data analytics, and the urgency of their claims on data analytics (see figure below). Power refers to the extent to which a stakeholder can impose its will in a relationship; legitimacy to the extent to which a stakeholder's actions are desirable, proper, and appropriate in a social system; and urgency to the extent to which stakeholder claims call for immediate action.



In big data analytics context, organizations have high power and urgency but varying degrees of legitimacy. Organizations have high power as they have the technology, data, and expertise necessary to engage in data analytics activities that impact individuals and society. They have high urgency because they complete much of their data collection, algorithmic decision making, and subsequent actions in short time frames in part due to competitive pressures (e.g., high-frequency trading on stock markets). Organizations have varying degrees of legitimacy depending on the extent to which their actions oppose the individuals' and societies' values. Thus, organizations have high salience and urgency in the big data analytics context, and one may consider them dangerous stakeholders when their actions have low legitimacy

Individuals engaged as stakeholders have low power and urgency but high legitimacy. Individuals have low power because they can rarely impose their will on other stakeholders involved and often do not know how organizations collect and use their personal data. They have low urgency because they participate in big data analytics rather passively and have relatively less need for immediate action. Individuals have high legitimacy because their actions are mostly desirable, proper, and appropriate in society. Inappropriate actions can lead to sanctions and legal consequences. Hence, individuals have low salience in this context, and one may consider them discretionary stakeholders whom other stakeholders frequently ignore. Society as a stakeholder has varying degrees of power, low urgency, and high legitimacy. Generally, societies impose their will through laws, regulations, guidelines, and sanctions. However, they cannot easily develop and implement such things in a context that features rapidly evolving technology and the need for consensus. Privacy laws, such as in particular the European Union's GDPR, exemplify societies' power. Societies have low urgency because developing and implementing policies, guidelines, and laws concerning big data analytics takes a long time, while technology and its use by organizations evolves rapidly. Societies have high legitimacy because their actions are generally desirable, proper, and appropriate for their citizens. Therefore, society has low salience, and one may consider it as a discretionary stakeholder whom other stakeholders frequently ignore.

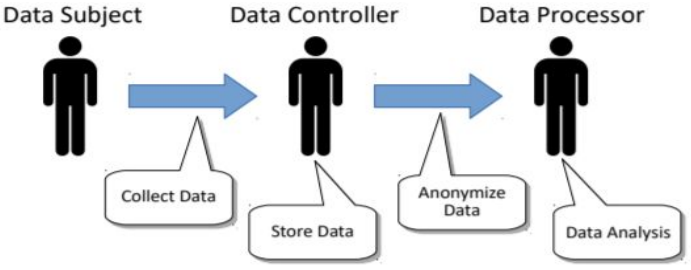
Interactions between Individuals and Organizations - To increase their salience in interactions with organizations, individuals need to increase their power and urgency. They can do so in several ways. Individuals need to become more knowledgeable about data and how it can be used. They must understand the practices and consequences of data and then interact with organizations to ensure that the organizations establish ethical governance practices and that they have more access to and control

over their personal data. Only then can individuals and organizations work together to ensure the quality of personal data and transparent data-trading practices. Furthermore, organizations need to develop decision-making practices that respect individuals' freedom of choice and further build trust and reputation. Increasing the salience of individuals in their interactions with organizations can lead to mutual benefits and, by enabling ethical discourse, more ethical big data analytics practices to emerge.

Interactions between Organizations and Society - To increase their salience in interactions with organizations, societies need to increase their power and urgency. Groups in societies must develop and implement effective principles and guidelines for organizations and, thereby, promote ethical governance practices. Societies should further develop these principles and guidelines into regulations and laws, such as national privacy regulations and laws, that they can use to sanction organizations that do not comply. As a society, we must find ways for organizations to engage ethically in data trading without subjecting society to Orwellian-level surveillance. Increasing the salience of societies in their interactions with organizations can lead to mutual benefits and, by enabling ethical discourse, cause data usage practices that balance different stakeholders' interests more ethically to emerge.

Interactions between Individuals and Society - Both individuals and societies need to increase their salience in interactions with organizations. Individuals should actively participate in developing principles and guidelines to ensure that societies establish regulations and laws with effective sanctions. Such sanctions will help to protect individuals' rights about data privacy and freedom of choice. Societies can provide education to help individuals better understand the benefits and costs of their data. Societies need to find ways to share in the benefits of big data analytics without coercing individuals to provide data in order to participate in society. Increasing the salience of individuals and societies jointly in their interactions with organizations can lead to mutual benefits and, thus, enable an ethical discourse and a strong impetus for organizations to develop and adopt better data usage practices.

Key stakeholders in Data management:



- Data Subject- Any person whose personal data you collect or process.
- Data Controller- The person who determines the purpose and methods for processing the data.
- Joint Controllers- Two or more controllers who jointly determine the purposes and methods of processing data.
- Data Processor- The person or company who processes data on the instructions of the controller.
- Data Sub-Processor- A third party individual or business which performs data processing for other companies, and is accountable for the data processed.
- Supervisory Authorities- Public authorities who monitor the application of GDPR.

Data Handling Process

Stakeholder Analysis Matrix:

High

Keep Satisfied Data Controllers (who determines the purpose and methods for processing the data)	Encourage and Influence Supervisory Authorities (who monitor the application of GDPR)
Monitor Data Processor (who processes data on the instructions of the controller) Data Sub-Processor (third party individual accountable for the data processed)	Keep Informed Data subjects (like customers, subscribers, users, employees, partners, external workforce)

Low Interest High

Value Conflict Analysis

Data is ubiquitous because it is so useful. This means that many different parties—data subjects and sources, associated communities, researchers, governments, and businesses—will have competing interests in relation to the data. Just as we make trade-offs in our daily life (to walk or to drive to work? doughnut vs. salad for lunch?), we need to make trade-offs about competing interests in relation to data.

Note that many parties who don't have legal rights to control access to and use of data, may nonetheless have compelling interests in the data. Responsible data use requires attention to these broad interests. Facebook's recent troubles highlight this. Even if Facebook was legally entitled to share users' data with Cambridge Analytica, Facebook massively underestimated users' interests and expectations in relation to privacy, control, and appropriate use.

In areas of rapid progress, such as data science, practice can quickly outstrip the legal framework. Data use may be within the parameters of the law (e.g., data protection or privacy regulation) but may nonetheless be unethical and/or outside the social licence. We should be aiming to align the social licence, ethics, and the law to ensure that data use is publicly acceptable, normatively justified, and legal. Where there is misalignment of the law, ethics, and the social licence, data users need to tread carefully.

eEthical deliberation

That can help identify who has an interest in the data and where these interests might clash; help data holders to articulate the ethical trade-offs that need to be made; and guide deliberation about responsible data use. The values often clash—maximizing data security will conflict with maximizing social value through broader data use. Under different circumstances, priority will appropriately be given to different values. This process is about making informed, explicit, and justifiable trade-offs, rather than following a set of prescribed rules.

Social value

Data is in demand because it has value. Data can contribute to knowledge and innovation, drive efficiency, reduce harm from ineffective or poorly targeted services, and reduce costs. Open data is important to drive the advancement of scientific knowledge, preserve datasets, test and verify conclusions, refine algorithms, and safeguard against misconduct.

Harm minimization

Data collection, storage, and use should be designed to minimize and manage risks of harm. Harms can be physical, economic, psychological, or reputational and can be experienced by individuals, communities, or organizations. Anonymization (pseudonymization and de-identification) has been the cornerstone of protecting individual data subjects from harm. However, anonymization is failing in the era of big data, where there are hundreds of thousands of data points for a single individual. Data scientists have proven repeatedly that they can re-identify individuals in supposedly anonymous datasets. Furthermore, anonymization and de-identification do little to protect communities from harm. Data analytics and artificial intelligence (AI) are increasingly used to characterize the behavior of communities and inform the delivery of services. Data can be used to stigmatize or discriminate.

Control

Control refers to the capacity for data subjects to be autonomous and self-determining. Were data subjects asked for their consent at the point of data collection? To what degree will data subjects' preferences determine how the data is used? Is this a secondary use of the data that differs from the original consent? Is the data use novel and original or is it likely to be consistent with the expectations of data subjects? Various models of consent have been proposed for data, including broad consent, dynamic consent, and meta-consent. However, much data use (especially linking and secondary uses) occurs without consent. In these cases, data users need to be safe stewards of the data. Transparency, engagement, and accountability are especially important for data used without consent.

Justice

Justice concerns the equitable treatment of those with an interest in the data activities, including the fair distribution of any benefits and burdens arising from the collection, storage, use, linkage, and sharing of data. The term "benefit sharing" was first used in relation to non-human genetic resources in the Convention on Biological Diversity adopted at the Earth Summit in Rio de Janeiro, Brazil, in 1992. Benefit sharing requires that the advantages/profits derived from the data are shared fairly among the data providers and the community from which the data originates. Recent data advocacy, especially in relation to indigenous data, has moved away from "benefit sharing" toward "power sharing," arguing that data subjects and communities should have decision-making capacity in relation to data governance and use.

Trustworthiness

Trustworthiness is the property of being worthy of trust. It can apply to individuals, organizations, and institutions but also relates to data quality, systems of knowledge production, scientific integrity, and professional standards. When judging trustworthiness, we look for truthfulness, reliability, and consistency but also goodwill. A robust data ecosystem requires a high level of trust. A breach of trust can affect not only the agents involved but an entire profession or institution. The dispute between Arizona State University and members of the Havasupai Indian tribe over the use of genetic samples

for research left a legacy of mistrust and fear of exploitation. As Tuhiwai Smith famously argued, "'Research' is probably one of the dirtiest words in the indigenous world's vocabulary". Trust, when lost, can take significant efforts to rebuild.

Transparency

Transparency is openness and accessibility in decision making and actions. When the data activity occurs without the data subjects' consent and is justified on the grounds of "social value," the arguments in favor of transparency and openness are especially compelling. Transparency helps to demonstrate respect for data subjects and trustworthiness, and it underpins public engagement and accountability. Full transparency would include a public description of the data activity, purpose and justification, anticipated social value, harm-mitigation strategies, public engagement strategies, level of security and encryption, research results, and the coding/algorithms. When launching a £1.5 billion initiative in AI in April 2018, France's President Macron announced that anyone receiving AI funding money from the government will be required to make their algorithms open and transparent.

Accountability

Accountability refers to holding data users and custodians responsible for the consequences of their decisions and actions. Data regulation is increasingly focused on accountability. A significant innovation in the EU General Data Protection Regulation (GDPR) (which came into force in May 2018) is the introduction of "accountability" (Article 5(2)) to the list of principles relating to personal data. Under the GDPR, organizations will need to be more intentional about their data collection and use and maintain open lines of communication with data subjects.

Conclusion

Given these competing values, there will be multiple different "ethical" solutions to data management. The task is to identify the ethical issues, reason through how to balance conflicting demands, articulate the trade-offs, and justify the conclusions. Do this as publically and transparently as possible, and make time to revise and re-assess.

We use data to tell stories, to make sense of the world. This means telling stories about people and how they live. Data has the appealing veneer of scientific objectivity, but the process of telling stories is never ethically neutral. Our starting point should be to ask: Where is the human in the data? What would this data use look like from the data subjects' perspective?

Proposed Innovative options:

Data generated through the use of these numerous smart devices are collected and stored by companies, which do not always act transparently. Terms of use and service are often extremely technical and unintelligible to the general population. It is not uncommon that the intended purpose of the data be hidden from the users themselves, who have no control over the information that refers to them. Given the voluminous amount of data produced daily, this becomes even more worrisome, especially since the "Big Data" phenomenon goes far beyond a tangle of data, being essentially relational. We must bear in mind that Big Data is us, and therefore we must have a critical conscience about it and think about possibilities to regain control over our personal data.

With ownership and availability of our data, companies use techniques such as targeting, tracking, and profiling to target their marketing policies to the way we live and our needs — or to what they make us believe to be a necessity. In this way, discussions about the right to privacy are inextricably linked to discussions about the use and management of data. The technological advance requires adaptations of the legal order to the new scenarios, which can happen, for example, through the legislative action or the interpretive activity. These solutions are not always effective: on the one hand, the sociopolitical conjuncture and the technological pattern change much more rapidly than legislation can accompany, and, on the other hand, paternalistic and cooperative distance from the will of individuals. Thus, new ways to protect the right to privacy and to increase the control that Internet users have about their own data have emerged as an alternative.

Individuals to whom the information refers to, do not even know in general purpose for which they are used, which creates serious privacy problems and fails to meet the principle of transparency.

In this sense,we propose a solution. It is basically a system whose objective is to place the individual at the center of personal data so that they themselves have control of the information produced about themselves, being free from the abusive control of data currently exercised by companies. It adopts a perspective centered on the human being, and no longer on the things or the information itself. In the current management model, the data is from those who collect it. Individuals to whom the information refers to, do not even know in general purpose for which they are used, which creates serious privacy problems and fails to meet the principle of transparency. The new system seeks to create a scenario in which users have their human rights respected in the digital environment and can control their data while creating barriers to business innovation that can develop based on mutual trust.

Hashing of confidential information

The metadata describing the (identifying) documents attested to on the Shyft chain is encrypted with a symmetric key shared by the trust anchor and the user whose data the attestation references. Not only does this keep this metadata confidential, it adds an additional layer of security. This is because documents in an attestation are referenced by a hash of the (possibly digitized) document, which is extremely difficult to guess without having access to the document itself.

When a data user seeks to demonstrate to a trust anchor that they have permission to access a document, the message that they send to the trust anchor is required to identify the documents whose sharing has been consented to, by this hard-to-guess hash. The hash is part of the data that’s encrypted with a symmetric key before being included with the attestation. This means that a consent message needs data unlocked by the data-owner/user’s key in order to be meaningful, in addition to requiring that the consent message be signed by the user/data-owner in order to be valid. It should be noted that the symmetric key is not included in the signed data; this allows the existence of signed consent to be audited, without having to share this (confidential) key with the auditors.

How end-users remain in control of their data

Furthering our commitment to ensure that our end-users are in control of their data (and working from the principle that if a piece of data is about you, that makes it your data, regardless of who collected, generated, or otherwise has custody of it), the Shyft consent messages include a field where the end-user giving consent can specify exactly what they’re allowing the recipient of the data to do with it. Some example uses include storing (or merely accessing) a copy of the data to comply with regulations (such as Know Your Customer rules), or verifying properties of the identity referenced in the data (e.g. that the person described isn’t a politically exposed person, nor do they count as an insider on any publicly traded company) and, optionally, to post an attestation making the results of that verification available.

We also expect that even where not required by the privacy regulations, we will provide strong incentives for application providers (possibly up to the point of being endorsed to offer their applications on the Shyft network at all) not to require users to consent to data uses that are neither necessary for the core functionality of the service being provided, nor for regulatory compliance. After all, consent is all but meaningless when granted under coercion, and this is not a state of affairs that we intend to promote.

Consent management
Another important feature of consent that we are implementing is the ability for this consent to be revoked. This is a more complicated feature to implement, as it can involve some degree of negotiation to determine whether, for example, data whose consent to store has been revoked can in fact be deleted without forcing an application provider into regulatory non-compliance. Although this is more complicated, and even though we could likely take advantage of broad interpretations of certain existing standards (e.g. the public interest exception in the GDPR) to avoid implementing these negotiations, we're including them anyway.

This is both a demonstration of our commitment to user privacy, and a challenge to other companies holding private data to comply with as strict an interpretation of the public interest exemption as we are adhering to.

Pathway and Justification:

Consumer activism
Consumer awareness and involvement will trigger a much greater conversation about what data privacy means, and how it is applied. If governments and organisations provided consumers with more ways of tracking how a company got their data from, and given more transparent information around individual rights, and easier processes to opt out and withdraw consent to data, the more healthier the conversation.
Awareness of trust will be raised between consumers and organisations. Data breaches, cold calling scandals, and data misuse court cases have all eroded the trust in for-profit and non-profit entities, so this needs to won back through transparency, and a candid relationship with consumers over how data is and is not being used.
Consumers also have the power to shape how regulators enforce sanctions for GDPR non-compliance. It would be impossible for organisations like the Office of the Australian Information Commissioner to monitor the entire Internet for breaches in the policy, so wronged citizens need to flag the issues that matter to them. While we're still waiting to see what transgressions lead to what fines, we should all exercise our rights to exert pressure on the regulator to meet public demand.

International coordination will remain patchy at best
In an ideal world, there would be an international standard for data privacy, however, this is unlikely due to the nature of each country and its government. This means that on a national scale, more work needs to be done to make sure the right rules are in place.
Although the Assistance and Access Bill has been amidst controversy lately, it's a step forward in putting regulations in place and a conversation driver between business, media and government in driving action against data privacy, far better than no action at all.

On the other hand, a lack of coordination on an international scale breeds complexity for Australian businesses who trade internationally. Even Australian universities have international students who must adhere to data regulations like the GDPR, but with the new encryption laws they can't guarantee complete data protection. This is why it is important for governments to work with their corresponding private sectors to canvas the best possible solution for all parties involved.

Ethical questions around automation

We are still in the infancy of any ethics discussions around how anonymised, once personal data is used and managed.

Firstly, with anonymised data, businesses are profiting from the use of a person's information, just without their name attached. Tap My Data is a great example of how consumers are getting a monetised piece of the action, and recent research suggests that Facebook users would want to be paid more than $1,000 to deactivate their accounts for a year.

Secondly, there is an ethical dilemma around anonymised data. A wearable health device can track heart activity which is then analysed, anonymously, by healthcare researchers using artificial intelligence (AI). If one finds a correlation between a certain reading and a healthcare risk, is there an ethical obligation to then inform users who exhibit this pattern?

If the data is anonymised, this isn't possible and the De-identification and the Privacy Act even expressly forbids efforts to de-anonymise data. How these types of issues get handled will likely remain a topic of debate for years to come, as deep learning and artificial intelligence (AI) generate more insight from increasingly sophisticated ways of collecting this sort of data.

Taking a more stringent approach to data protection inevitably leads to better data management overall, which means that businesses can save money and use their data more efficiently to solve business challenges. At the same time, customer trust is earned and built.

It's exciting to see what the future of data privacy will include, particularly as businesses make an active, long-term commitment to privacy and ultimately, rebuilding trust with their customers. Ethical questions will continue to be asked, but for good reason. This will only lend to more comprehensive regulation around data use and management.

REFERENCES

1. **https://blog-sap.com/analytics/2017/09/07/gdpr-a-closer-look-at-a-companys-stakeholders-and-their-obligations/**
2. **https://aisel.aisnet.org/cgi/viewcontent.cgi?article=4140&context=cais**
3. **https://pdfs.semanticscholar.org/1e83/14c448111163ed405567eaddc30ac273a462.pdf**
4. **https://www.youtube.com/watch?v=KYfADOlstwc&list=RD4ZHwu0uut3k&index=2**
5. **https://arxiv.org/pdf/1811.08531.pdf**
6. **https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf**
7. **https://www.digitalistmag.com/cio-knowledge/2017/09/19/gdpr-closer-look-at-companys-stakeholders-obligations-05353543**

8. https://www.insideprivacy.com/data-privacy/ntia-publishes-stakeholder-comments-on-consumer-privacy-proposal/
9. https://www.darzin.com/blog/gdpr-are-you-ready
10. https://www.accenture.com/in-en/insight-data-ethics
11. https://www.isaca.org/Journal/archives/2016/volume-6/Pages/an-ethical-approach-to-data-privacy-protection.aspx
12. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
13. https://www.ibe.org.uk/userassets/briefings/ibe_briefing_62_beyond_law_ethical_culture_and_gdpr.pdf
14. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf
15. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1365-2648.2010.05563.x
16. https://www.researchgate.net/publication/226528834_Privacy_in_the_Information_Age_Stakeholders_Interests_and_Values
17. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6047448/
18. https://www.itgovernance.co.uk/blog/what-is-data-protection-by-design-and-default
19. https://aisel.aisnet.org/cais/vol44/iss1/34/
20. https://blog.infinitydirect.com/2018/12/05/intelligent-data-privacy-management-and-consent-compliance-for-marketers/
21. https://www.iqvia.com/blogs/2018/10/data-privacy-consent-collection-and-management
22. https://www.unglobalpulse.org/privacy-and-data-protection-principles