

Digital Ethics

Insights into how technology shapes us and the world we live in



THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

Submitted by:

(401903022) ADITYA UPADHYAY

(401903030) AKSHAT RAI

(401903002) VARNIKA SINGH

(402083002) HITEN MITTAL

BE-MBA Third Year, CoEM

Under the Guidance
of

Mr. Mohit Taneja

**Thapar Institute of
Engineering and Technology**

ABSTRACT

From the manner in which we work to the manner in which we mingle, innovation has practically changed every part of our general public in the course of recent years. In the event that we investigate how our youngsters today play and interface versus the age previously, we will locate that the more significant part of the kids matured between two and five years that can run applications and computer games yet can't tie shoelaces or ride a bicycle. Startling right? Well, not exactly. The ever-increasing advancement in technology in today's world and the involvement of the individuals in these advancements have led to individuals getting distant from manual work and labour and moving more towards automation. But while this automation has eased our everyday lives, it does have many drawbacks associated with it, one of the biggest being that our lives now live on the internet.

This affects all aspects of our lives, whether it is autonomous devices that collect our information while we go about our day, or our social media accounts where our precious information is sold on the internet for a couple of dollars. All this data flow has a huge impact on our lives as information that we may not have wanted to share with the wider world can still be taken and made available without our informed consent.

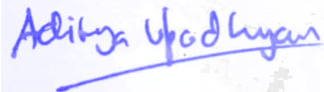

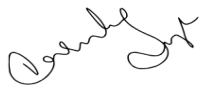

This means that even without hacker groups creating major cyber-attacks on sensitive information, our data remains vulnerable on the internet and is at the mercy of the companies that we have trusted to protect them. While these companies have shaped our lives in ways that have improved them vastly, the question that arises for many is where we draw the line.

The concept of digital ethics focuses on the various aspects of our lives which are now dominated by technology and how we as a society need to step up and hold not only the technology giants responsible to use the data in an ethical fashion but also inform people about how they can protect themselves from the evils of the internet, by making them aware of the things that they should and should not share on the internet and how to protect the information that they have shared.

DECLARATION

We hereby declare that the report entitled **Digital Ethics** is an authentic record of original work carried out under the Humanities & Social Sciences Department, TIET, Patiala, under the guidance of **Mr. Mohit Taneja**, 6th semester (2022).

Date: 22/05/22

Roll No.	Name	Signature
401903022	Aditya Upadhyay	
401903030	Akshat Rai	
401903002	Varnika Singh	
402083002	Hiten Mittal	

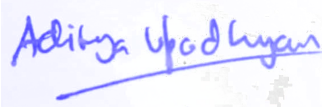

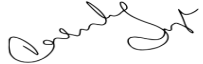

ACKNOWLEDGEMENT

We would like to express our thanks to our mentor Mr. Mohit Taneja. He has been of great help in our venture, and an indispensable resource of knowledge. He is truly an amazing mentor to have.

We are also thankful to Dr. Anupam Sharma, as well as the entire faculty and staff of the Humanities & Social Sciences Department, and also our friends who devoted their valuable time and helped us in all possible ways towards the successful completion of this project. We thank all those who have contributed either directly or indirectly towards this project.

Lastly, we would also like to thank our families for their unyielding love and encouragement. They always wanted the best for us and we admire their determination and sacrifice.

Date: 22/05/22

Roll No.	Name	Signature
401903022	Aditya Upadhyay	
401903030	Akshat Rai	
401903002	Varnika Singh	
402083002	Hiten Mittal	

LETTER OF TRANSMITTAL

May 22, 2022
Mr. Mohit Taneja
Research Scholar
Thapar Institute of Information and Technology
Bhadson Rd, Adarsh Nagar, Prem Nagar
Patiala, Punjab 147004

Dear Mr. Mohit,

This report is an analysis on the various aspects of our digital lives and the role various large technology companies play in shaping not only our digital lives but also our real lives. We have collected information about various fields where digital ethics are being questioned by experts and where the borders between privacy and convenience seem to merge. The report also contains a number of statistics regarding the estimated cost and amount of data that is said to be in motion around the world. We have put in our teams personal views as well as the views of experts on the subject matter that can allow us to shape a better future for the world of technology which is based on the use of proper ethics by not only the companies but by the users as well.

Aditya has cross-examined all the technical knowledge that is part of the report while Varnika helped in giving the report a proper conclusion. Hiten was responsible for the introductory part of the report. Akshat, has double-checked all the facts and figures that have been mentioned in the report and was responsible with the entirety of the team for putting this document together.

We hope this report meets your needs, generates future studies, and educates the public about digital ethics that not only they should follow but they should push the technology giants to comply with to.

If you have any further queries feel free to contact Team Digital Ethics at krishita81@gmail.com .

*Sincerely yours,
Team Digital Ethics
Thapar Institute of Information and Technology*

LIST OF FIGURES

Figure No.	Caption	Page No.
Figure 1	Data is New Oil Bar Graph	6
Figure 2	Data is New Oil World Map	6
Figure 3	Data Blockage World Map	6
Figure 4	Data Awareness stats	7
Figure 5	Emotional Data Awareness stats	7
Figure 6	Data Protection World Map	7
Figure 7	GDPR awareness World Map	8
Figure 8	GDPR awareness Company Stats	8
Figure 9	Company Investment in Data Protection	8
Figure 10	Cambridge Analytica Scandal Stat (1)	9
Figure 11	Cambridge Analytica Scandal Stat (2)	9
Figure 12	Data Breach Financial Stats	9
Figure 13	Cambridge Analytica Scandal Stat (3)	10

TABLE OF CONTENTS

ABSTRACT...	ii
DECLARATION...	iii
ACKNOWLEDGEMENT...	iv
LETTER OF TRANSMITTAL	v
LIST OF FIGURES	vi
CHAPTER...	Page No.
1. INTRODUCTION	1
2. LITERATURE REVIEW	2-3
3. OBJECTIVES OF STUDY	4
4. RESEARCH AND DESIGN TECHNOLOGY	5
5. DATA ANALYSIS	6-10
6. INTERPRETATION	11-13
7. DISCUSSION	14-15
8. CONCLUSION	16
9. RECOMMENDATION	17
APPENDIX A: References	

INTRODUCTION

As the world is becoming more modern, digital activities are on the rise, and this time, at an all-time high rate. Education, charities, and services are becoming increasingly driven by data and expanding their digital activities to encompass service delivery, fundraising, marketing and communications, and accessibility.

According to Wikipedia, digital ethics is defined as “the branch of ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, and use of information, and the ethical standards and moral codes governing human conduct in society”.

Every picture we upload, every post that we publish, every card swipe, all gets stored somewhere in the world in the servers and into the bloodstream of the internet. How do we know the data we share is secure? Can we ask Google, or Facebook about how many data points of an individual are stored with them, or, what data is stored with them even after the deletion of the data from our side? How much of our data is shared or sold, these questions remain unanswered, and we people who use the internet need to be aware of how data is stored and how much privacy is being taken care of by these giants.

This report dives into the study of how data is used and its value by using demographic and psychographic statistics and analysis of it, making meaningful observations and drawing important conclusions.

LITERATURE REVIEW

Digital Ethics: Rhetoric and Responsibility in Online Aggression

Digital Ethics delves into the shifting legal and ethical landscape in digital spaces and explores productive approaches for theorizing, understanding, and navigating through difficult ethical issues online.

Contributions from leading scholars address how changing technologies and media over the last decade have both created new ethical quandaries and reinforced old ones in rhetoric and writing studies. Through discussions of rhetorical theory, case studies and examples, research methods and methodologies, and pedagogical approaches and practical applications, this collection will further digital rhetoric scholars' inquiry into digital ethics and writing instructors' approaches to teaching ethics in the current technological moment.

Digital Ethics: Research and Practice

In a digital age of perceived anonymity and diminishing face-to-face contact, what does it mean to be true to oneself? Has the internet given us the license to be false to others, without consequence? Technology has given us capabilities we previously did not have and changed the way we think about time and space.

Although research is now being done on many aspects of the interplay between humans and technology, there currently exists a vacuum regarding behaviour and usage of technology. This edited volume contains some of the best research on digital ethics from authors in communication, law, information studies, education, philosophy, political science, computer science, and business on topics that range from sexting to piracy.

The Ethics of Digital Well-Being: A Multidisciplinary Perspective

serves as an introduction to the edited collection of the same name, which includes chapters that explore digital well-being from a range of disciplinary perspectives, including philosophy, psychology, economics, and health care, and education. The purpose of this introductory chapter is to provide a short primer on the different disciplinary approaches to the study of well-being. To supplement this primer, we also invited key experts from several disciplines—philosophy, psychology, public policy,

and health care—to share their thoughts on what they believe are the most important open questions and ethical issues for the multi-disciplinary study of digital well-being. We also introduce and discuss several themes that we believe will be fundamental to the ongoing study of digital well-being: digital gratitude, automated interventions, and sustainable co-well-being.

IJSER

OBJECTIVES OF THE STUDY

The objective is to focus on ethical problems posed by the collection and analysis of large datasets and on issues ranging from the use of Big Data in biomedical research and social sciences to profiling, advertising, data donation, and open data.

In this context, key issues concern possible reidentification of individuals through data-mining, –linking, –merging, and re-using of large datasets, and risks for so-called “group privacy”, when the identification or profiling of types of individuals, independently of the de-identification of each of them, may lead to serious ethical problems, from group discrimination (e.g. ageism, racism, sexism) to group-targeted forms of violence, trust and transparency are also crucial topics, in connection with an acknowledged lack of public awareness of the benefits, opportunities, risks, and challenges associated with the digital revolution.

For example, transparency is often advocated as one of the measures that may foster trust. However, it is unclear what information should be made transparent and to whom information should be disclosed.

The demanding task of digital ethics is navigating between social rejection and legal prohibition in order to reach solutions that maximize the ethical value of digital innovation to benefit our societies, all of us, and our environments.

We have come to understand that it is not a specific technology (now including online platforms, cloud computing, Internet of Things, AI, and so forth), but the whole ecosystem created and manipulated by any digital technology that must be the new focus of our ethical strategies. The shift from information ethics to digital ethics highlights the need to concentrate not only on what is being handled as the true invariant of our concerns but also on the general environment (infosphere), the technologies and sciences involved, the corresponding practices and structures (e.g. in business and governance), and the overall impact of the digital world broadly construed.

RESEARCH AND DESIGN TECHNOLOGY

Today, digital transformation is the biggest driver of growth for organizations. Organizations are continuously focusing on implementing strategies for a better customer experience, operational efficiency, employee engagement, and new business models. In this paradigm, there is a focus on people, processes, and technologies. While the growth in technology is unprecedented, what is interesting is how the change in processes and people has ensured that organizations get the most out of their investments.

Ethical management of this process affects autonomy and honor/dignity/respect of people in the digital world. As the boundaries between the digital and the real world continue to blur, this turn will have a huge impact on the real world of a person. Let us say that Bank A decides to use machine learning to decide who is accepted for a loan. Machine learning will need training on a data set, which could be historical data or user-created data.

If historically, the bank has denied loans to a certain category of people, the same bias would carry forward to the machine. So essentially, we have transferred our bias to the system and now the system would deny loans to that certain category of people. If we use a user to create the data to train the system, he might introduce this bias himself to ensure that a certain category of people was denied loans. Both these cases fall under the purview of digital ethics. In a recent speech, Masayoshi Son of Softbank said that in the near future the earth would be co-inhabited by humans and machines.

We may soon see a world with 10 billion people and 10 billion robots. This, in other terms, is the singularity, where each robot is connected to another robot. In that context, this becomes even more important as we may end up transferring our local biases to the machines. Those biases will permanently render some individuals outside the purview of services and facilities rendered by these robots.

DATA ANALYSIS

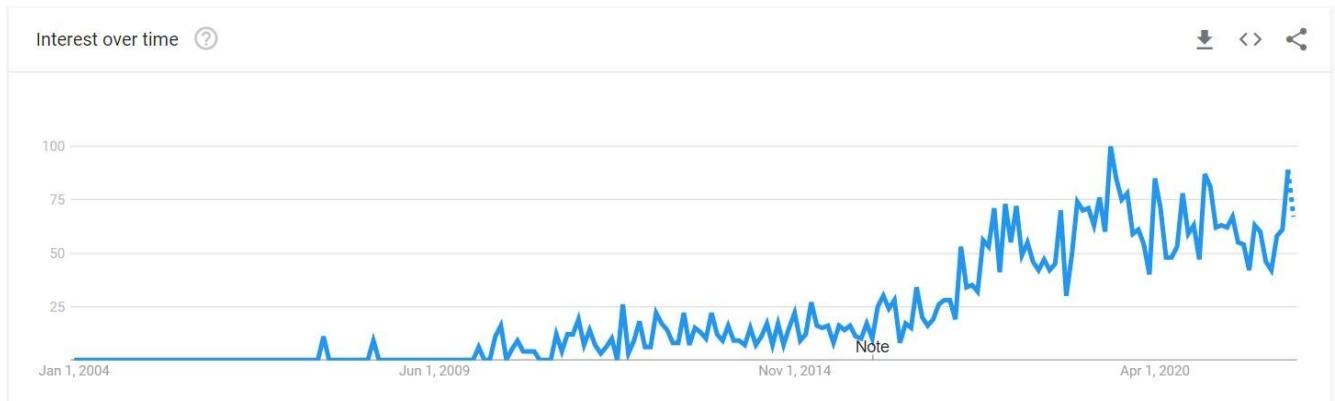


Figure 1- The graph presented above shows the use of the term “data is the new oil” around the world in Google searches and has been picked up using google trends [10]

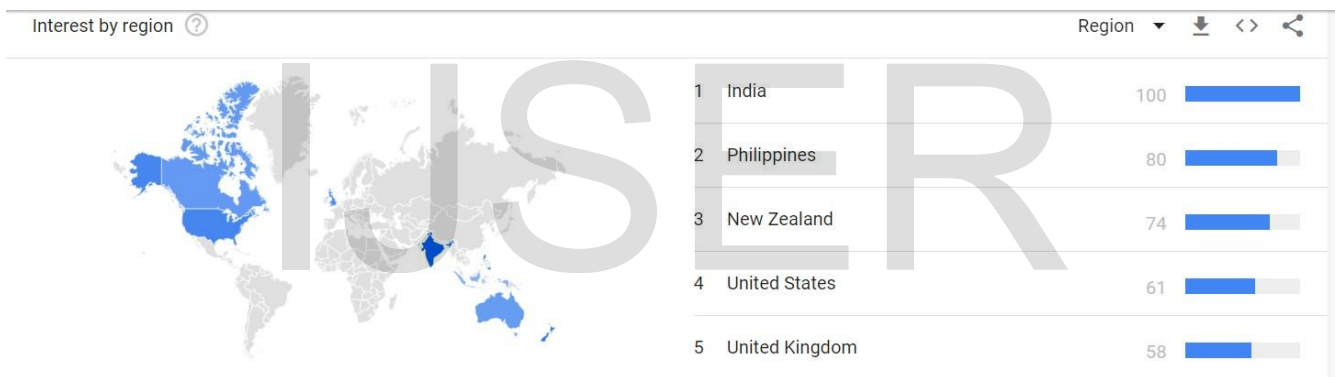


Figure 2- The map presented above shows the use of the term “data is the new oil” by various countries of the world in Google searches and has been picked up using google trends [10]

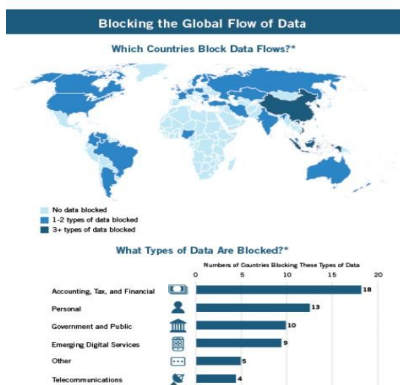


Figure 3- The map present on the side shows the stoppage of data flow by major countries and the kind of data that is blocked [11]

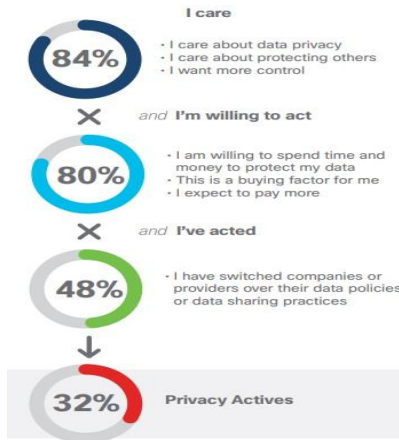


Figure 4- The image present on the side shows how many people are aware of various aspects of data privacy, the number of people willing to act on it and the number that are actually acting on protecting their data. [1]

		Companies	The government
Lack of control	They have very little/no control over the data ___ collect(s)	81%	84%
Risks outweigh benefits	Potential risks of ___ collecting data about them outweigh the benefits	81%	66%
Concern over data use	They are very/somewhat concerned about how ___ use(s) the data collected	79%	64%
Lack of understanding about data use	They have very little/no understanding about what ___ do/does with the data collected	59%	78%

Figure 5- The Infographic presented on the side shows how people feel about the current control that they have over their data. [3]

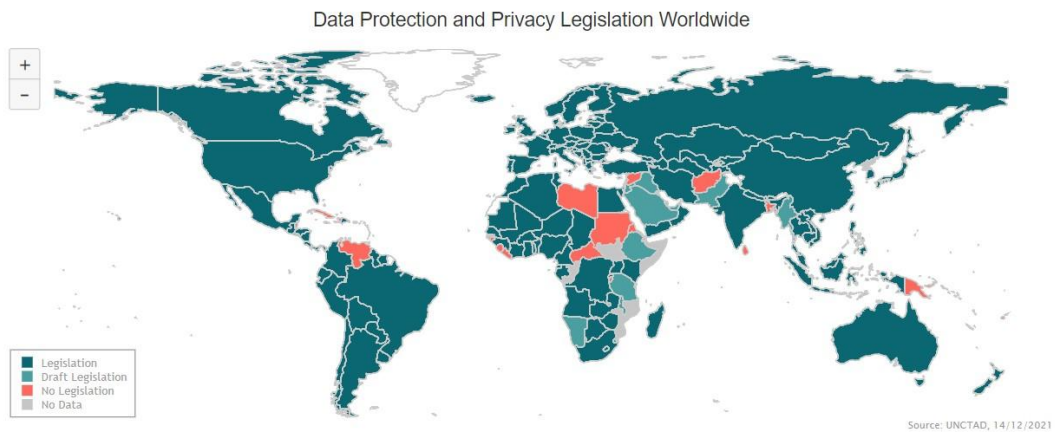
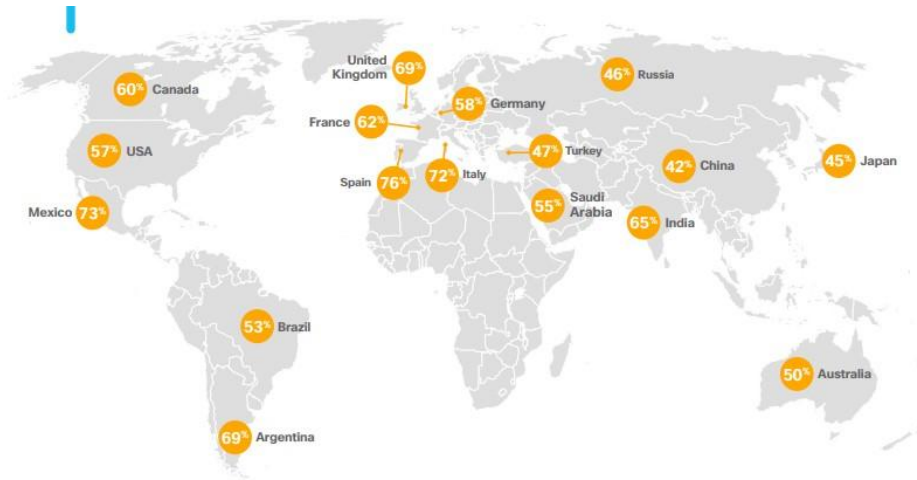


Figure 6- The map presented above shows the presence of data protection and privacy legislation that are in effect around the world. [5]



Source: Cisco 2019 Data Privacy Benchmark Study

Figure 7- The map presented above shows the number of people currently aware of the GDPR standards. [6]

What are the most difficult GDPR obligations in 2019

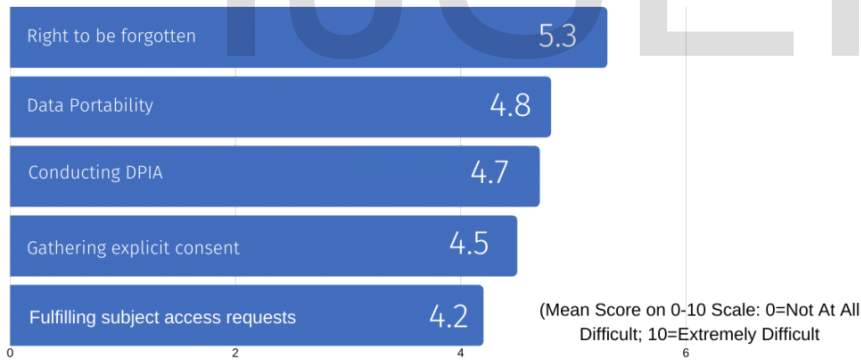
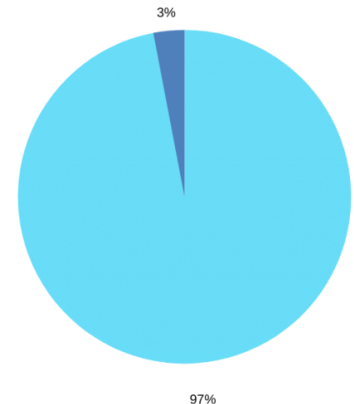


Figure 8- The Infographic presented on the side shows how companies feel about the current GDPR and what they find difficult in terms of application [15]

Figure 9- The Infographic presented on the side shows how companies feel about the investments that they have made in terms of privacy of customer data [6]

97 %

of companies recognized benefits such as competitive advantage from their privacy investments



Did Facebook sharing user data with Cambridge Analytica make US users concerned about how their information is used online?

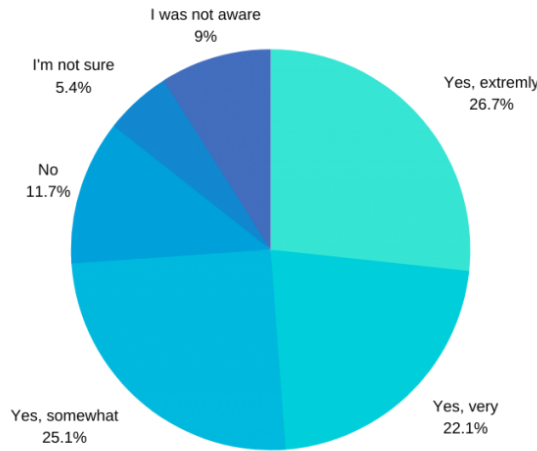


Figure 10- The Infographic presented on the sideshows customer reaction to the Cambridge Analytica scandal [7]

Figure 11- The Infographic presented on the sideshows customer reaction to the Cambridge Analytica scandal [7]

Could you forgive a company that falls victim to a data security breach if it immediately informs you about the attack and what it's doing to protect you?

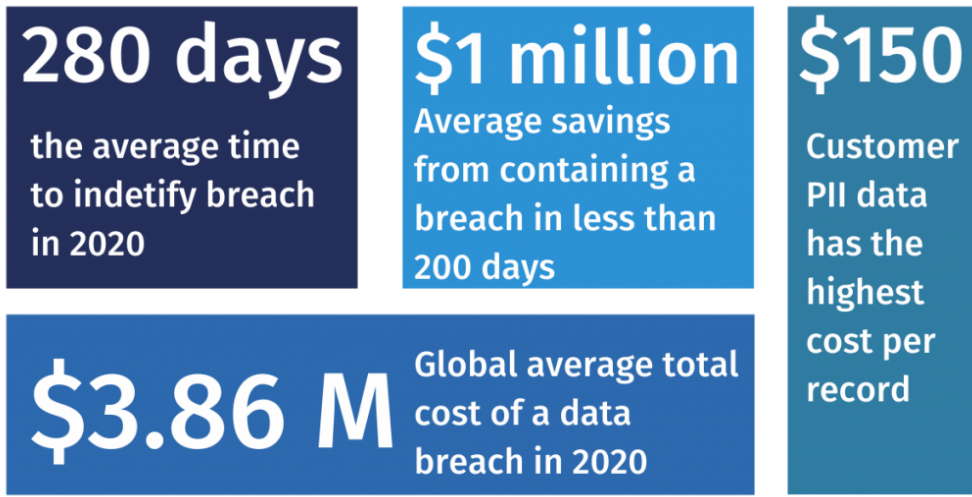
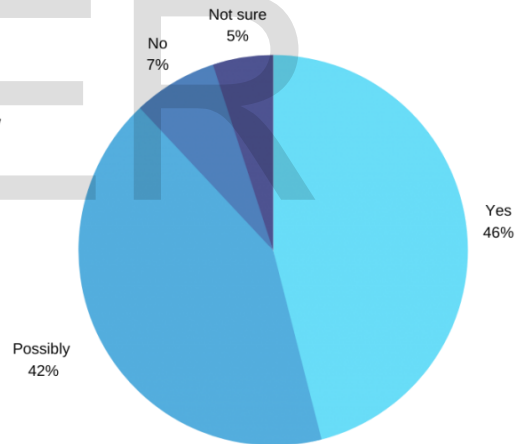


Figure 12- The Infographic presented on the side shows the economic effect of data breaches [15]

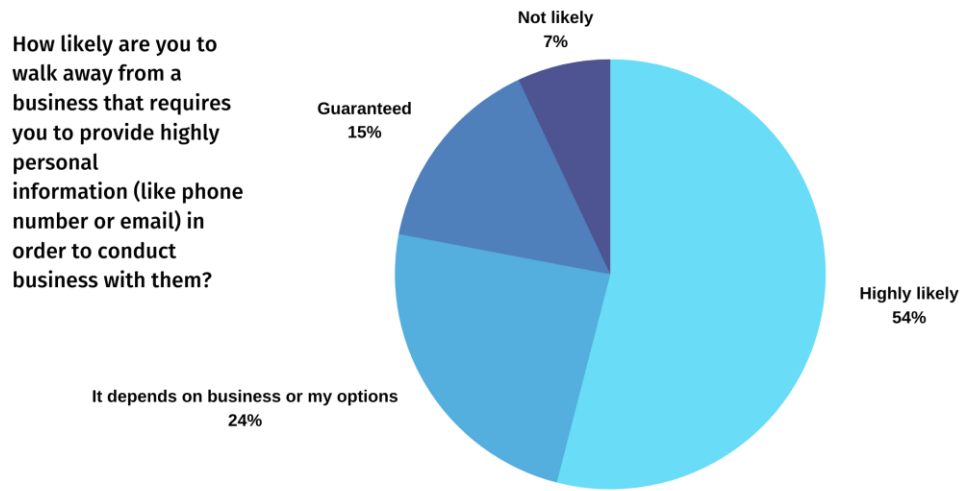


Figure 13- The Infographic present above shows the behavior of people towards businesses that have a high-security level. [\[16\]](#)

IJSER

INTERPRETATION

Figure 1- The huge flow of data means that data has become a currency of its own and is often being referred to as *the new oil* and is said to have a never-ending lifetime as while oil is a limited commodity, data has no end to it. This makes it a highly-priced commodity and sought after around the world. [\[10\]](#)

Figure 2- This fact is not only highlighted by the number of searches from around the world, which shows that India is leading this race, as it is the highest quoted search by country in the world, even overtaking the technology giant homes of the US and China, showing a high inclination of the current population to use the data that is currently being flowing around in the domestic and international market. [\[10\]](#)

Figure 3- One of the harsher steps being taken by governments around the world to stop data branches has been the blockage of dataflow by banning websites, and apps rampant along with banning data from and to certain regions altogether, leading to a significant amount of issues and inconvenience to the people present in such regions

Figure 4- Surveys conducted in the recent past have shown that people are starting to have an increased amount of awareness about their data and it's security and are willing to act to protect it from unauthorized usage. This means that companies now have to not only offer services but also be answerable to customer demands for ensuring the safety of their data, opening up a new market segment for data security firms. [\[1\]](#)

Figure 5- While there has been increased awareness about data privacy, the majority of the people feel that they are not in control of how their data is being collected and believe that it is the government and private companies that control their data and privacy. [\[3\]](#)

According to a survey conducted by Business news daily in the year 2021, 77% of respondents have heard about how companies use data to create targeted ads which makes the customer highly vulnerable and open to manipulation. [\[4\]](#)

Figure 6- More than 29% of countries in the world do not currently have any data protection laws in place to protect customers from technology giants exploiting their data. While 71% of the nations do have some sort of legislation in place, most nations have legislations that are not to date with the current technological advancements, meaning that these legislations more often than not provide citizens with enough protection. [5]

Figure 7- The world needs to have better data protection laws, one such example of a central rule regulation is the European Union's General Data Protection Regulation (GDPR) which applies to all businesses that reside in the EU. The figure tells us how world businesses are still not ready to comply with the regulations that are presented. [6]

According to a survey done by Data security firm Egress, more than 35% of US-based firms were not willing to completely comply with GDPR standards for data privacy as they felt it was too expensive to upgrade security. [7]

Figure 8- While GDPR has a number of benefits that can ensure an ethical internet working for most people around the world, companies are still reluctant to adopt it due to a number of economical and logistical issues that they feel they will have to operate with if they abide by the GDPR. [15]

Figure 9- With most companies reluctant to adopt the GDPR, almost all companies agree that it is a good investment if they invest in data security and privacy of customer data. [6]

Figure 10- The Cambridge Analytica leak has created a large buzz among everyone and the trust in Meta and all its subsidiaries seems to have taken a large hit with people now unwilling to trust the company to keep their data safe. [7]

Figure 11- But hope may not be completely lost as people still are willing to forgive the company for its mistake if it is willing to improve its current data policy and ensure that an activity like this does not get a chance to repeat itself. [7]

These surveys have allowed creating a sense of awareness among the people which has resulted in a number of positive outcomes, such as more than 65% of users surveyed by DuckDuckGo have claimed to have adjusted their data privacy settings on their browser [8], 90% of which is currently dominated by Google Inc. [12]

This number has also trickled down to social media users as well, with 80% users said to have changed their data privacy setting on their various platforms[8], which is majorly owned by Meta (formerly Facebook). [12]

The Cambridge Analytica scandal revealed the various vulnerabilities that are still present in the system, which resulted in 73% of people becoming concerned about how their information is being used on the internet [7]. 41% of customers believe that the company does not care about the data that they share with the company. [13]

Figure 12- The number of breaches and data attacks happening have had a huge impact on the entire world. While these attacks on data are detrimental to the customers, they also take a toll on the company, with an estimated attack every 39 seconds taking place on customer data worldwide [9] which accounts for an average of \$150 for every attack made [14], which results in billions of dollars worth of damages that companies have to suffer each year, with attacks only growing further and further in number. [15]

Figure 13- All of this information and better awareness from customers has had a huge impact on the customer psychology as they now not only are concerned with getting services but getting it from people that they can trust with the security of all of their vital information and are even willing to pay more for it. This has resulted in customers preferring to go with brands that ensure data security over others, with over 72% being in favor. [13]

DISCUSSION

“Privacy is dead, and social media holds the smoking gun.” – Pete Cashmore, CEO of Mashable.

Ever posted a photo of yourself, geotagged a post, or messaged someone about something you’re thinking of buying? It's unlikely you recall something like that right?

Well, the internet can.

Once you put something out there it's there forever, and it's probably far more valuable to big companies than you can comprehend. The fact of the matter is simple, our data is more valuable in today's world than almost anything else. The real question is what can we do about it, and should we do anything about it at all. Yes, our data is being collected constantly, and yes, most of it is collected without our knowledge. And given that we agree to massive and comprehensive terms of service documents that no one has ever actually read except for the lawyers that drafted it, we have no legal recourse.

But is that necessarily such a bad thing? One of the strongest arguments against data security regulation is that the companies are using the data for our own good. They are using it to optimise our experience, and make our lives easier. But the fact of the matter is, they’re doing it without our consent. We may have agreed to outrageous breaches of privacy on paper, and legally speaking, it is our fault, we should read a document before signing it. But that won't actually be enough. Terms of Service documents are purposely made to be ambiguous and confusing, they are full of obscured meaning and rhetoric. The kind of wording that no one other than an experienced lawyer could really make sense of. But it's still legal, isn't it.

All of this may be confusing, is there really no solution, and if there is should we enact it? If companies stop collecting our data, user experience will be significantly worse. No more Netflix recommendations, no more Spotify daily mixes, no more ads of exactly the product you were looking for on discount on Amazon. Are we willing to sacrifice this in order to protect our data? The companies have had our data for years already, it's not like they’ve all done bad things with it. Sure there are some bad apples like Facebook and Cambridge Analytica that exploited user data, but that doesn't mean everyone will be like them.

But here's the thing about bad apples, one or two spoil the entire lot. While the Cambridge Analytica leaks exposed Facebook's wrongdoings to the general public, they also sent a very clear message to other companies. The message being that your data is far more valuable than they thought, and given that Facebook faced little to no repercussions, The message is prefaced by the fact that companies can do whatever they want with your data and face no consequences.

In the end, we leave you with this thought. Think of Whatsapp, it has no actual revenue-generating product, so how does the company function? The answer is data. Whatsapp may be a messaging app, but it's a data brokering business. Now that isn't entirely unusual for a messaging service, the real question arises when you realise the fact the Whatsapp messages are End2End encrypted, meaning no one can see the messages except for the sender and recipient. So what data is Whatsapp selling? We don't know, and we likely never will.

IJSER

CONCLUSION

The current state of digital ethics and regulation are starkly bleak, with little to no security guaranteed to the consumer and their data. There have been some regulatory attempts through instruments such as the Belmont Report and GDPR, but these face two major issues, firstly they are either not put into effect to any degree, or only enacted at a local scale, and secondly, none of them actually address the root of the issue. They set guidelines for companies on how to collect and store data and what they can do with that data, but as has been the case with guidelines in all of history, there are always loopholes. And most companies that have our data also have more than enough resources to find and exploit those loopholes.

What we need is not weak, poorly worded regulation on data usage. We need regulation on public education. Far more important than forcing companies to limit data collection and usage is forcing them to inform consumers of what data is being collected and how it's being used. And then offer the user the choice to have this data collected if they want to. This needs to be done through clear and concise messaging intended to be understood by an ordinary consumer with no legal education. Only when the consumer has an understanding of the company's data practices and the option to opt into them, can they claim true ownership of their own data.

Only once the above regulations are enacted can we move on to storage and usage oversight. Under this context companies should be required to have external oversight committees to monitor data usage to make sure none of the consumers rights are breached in any way and there should be a limited amount of time for which any data can be stored after which it should be erased. Another very important component of any regulation should be consequences. Companies should receive massive sanctions and fines for breaches of the proposed regulation rather than a light slap on the wrist. Without stern consequences, regulation has no meaning whatsoever.

RECOMMENDATION

Based on the contents of this report we can make the following recommendations.

- Current digital ethics regulations are weak and unreliable and need to be dismantled to make way for stronger more effective regulations and oversight.
- The primary objective of any digital ethics and data rights regulation should be consumer education and autonomy rather than data usage and control oversight.
- Companies should be required to have external oversight committees to monitor data usage and ensure none of the consumers rights are being breached.
- Companies should only be allowed to keep user data for a limited amount of time, subject to the nature of the product and usage of the data.
- Consequences of any breach of regulation should be massive fines and sanctions and even criminal investigations in case of willful breaches.

REFERENCES

[1] Insight 1- People care about privacy, and a surprisingly large number have already taken actions to protect it , (November 2019) *Cisco Customer Privacy Survey*

https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf

[2] Insight 2- Privacy regulation provides “guardrails” for innovation and helps build trust, (November 2019) *Cisco Customer Privacy Survey*

https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf

[3] Americans and Privacy- Concerned and confused and feeling a lack of control over their personal information, (June 2019) *Pew Research Center*

<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>

[4] How Businesses Are Collecting Data And What They’re Doing With It, (December 2021) *Business News Daily*

<https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>

[5] Data Protection and Privacy Laws Worldwide, (December 2021) *United Nations Conference on Trade and Development*

<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

[6] Results- GDPR headlines , (January 2019) *Cisco Data Privacy Benchmark Study*

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf

[7] Data security survey (October 2019) *Egress*

<https://www.emarketer.com/content/with-ccpa-days-away-many-companies-are-still-not-compliant>

[8] Data security survey (October 2019) *DuckDuckGo*

<https://spreadprivacy.com/people-taking-action-on-privacy/>

[9] Micheal Cukeir, Hackers attack every 39 second (February 2007) *A James School of Engineering*

<https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>

[10] Google Trends (May 2022) *Google Incorporation Private Limited*

<https://trends.google.com/trends/?geo=IN>

[11] Nigel Cory, Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?

(May 2017) *Information and Technology and Innovation Foundation*

<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

[12] 100 Data Privacy and Data Security statistics (2020) *Data Privacy Manager*

<https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/>

[13] State of the Connected Customer Report Outlines Changing Standards for Customer Engagement

(June 2020) *Salesforce*

<https://www.salesforce.com/news/stories/state-of-the-connected-customer-report-outlines-changing-standards-for-customer-engagement/>

[14] _Cost of Data Breach Report (2020) *IBM Ponemone institute research*

<https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>

[15] IAPP-EY Annual Privacy Governance Report (2021) *iapp*

<https://iapp.org/resources/article/privacy-governance-report/>

[16] Consumer Attitudes Toward Data Privacy Survey (2021) *Akamai Research Institute*

[17] Digital Ethics : Rhetoric and Responsibility in Online Aggression

<https://www.routledge.com/Digital-Ethics-Rhetoric-and-Responsibility-in-Online-Aggression/Reyman-Sparby/p/book/9781032177571>

[18] Digital Ethics: Research and Practice

<https://www.luc.edu/digitaethics/researchinitiatives/essays/archive/2019/cdeppublicationdigitaethicsresearchandpractice/>

[19] The Ethics of Digital Well-Being: A Multidisciplinary Perspective

<https://link.springer.com/book/10.1007/978-3-030-50585-1>

IJSER