ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | May 2023
ISSN: 2582-6433

CONSUMER AND DATA BREACH IN DAY TODAY LIFE OF CONSUMER

AUTHORED BY - SANDHIYA KRISHNAN.S
& KARUNAMBIGAI.S
SASTRA DEEMED UNIVERSITY THANJAVUR

ABSTRACT

Customer data is information gathered from customers for a variety of purposes. They must now provide their private information, like their phone number and email address, everywhere they go. Furthermore, these data are probably going to be exposed via the same network, obtained unlawfully by hackers, or subjected to a cyberattack. Consumers may suffer from financial loss, loss of privacy and trust, identity theft, as well as harm to their mental health because of this data breach. Consumers must take action to avoid the breach of their personal data, in addition to the efforts that businesses should take. This article examines how data breaches have been handled in India and other nations, as well as what customers may do to safeguard their personal information.

KEYWORDS

Data breach, cyber-attack, loss of trust, data privacy, consumers

1) INTRODUCTION

Consumers must be concerned about data privacy because it pertains to the safeguarding of their private information, including name, address, phone number, and financial information, against unauthorized access, use, or disclosure. It is more important than ever to protect personal data as customers rely more and more on digital technologies and online services, making such data more vulnerable to exploitation.

Customers have the right to anticipate that businesses and organizations managing their data would

ISSN: 2582-6433

handle it with the utmost care and respect. The failure of businesses to protect the personal information of consumers can have serious repercussions, including legal action, reputational damage, and financial loss. To safeguard consumer data and foster customer confidence, businesses must put in place strong data privacy policies and procedures.

Consumers are now required to provide their personal information, such as their email address and phone number, either when purchasing a product (in stores or online) or while using a service that requires downloading an app on a mobile device. The compromise of their data, not the information they obtain, is the true issue. The protection of personal data, such as names, addresses, phone numbers, and financial information, against illicit access, use, or disclosure is a crucial concern for customers. More than 50% of Indian customers reported receiving unwanted offers from financial service providers after having their contact information made public due to a data breach. They consequently received a barrage of unsolicited proposals, including loans, insurance, etc., as per a survey. Reviewing privacy rules, adopting secure passwords, and exercising caution when disclosing personal information online are just a few measures that consumers may take to preserve the privacy of their data. In accordance with data protection legislation, they can also exercise their rights, including the right to access and modify their personal data.

In the final analysis, consumers place a high value on data privacy, so businesses must take the appropriate precautions to safeguard the personal information of their clients. Customers should be aware of the dangers and take precautions to protect their privacy when using online services.

2) HOW CONSUMER ARE BREACHED

a) SUPERMARKET

In a supermarket's unauthorised access to or disclosure of private customer information is referred to as a data breach. Personal data including names, addresses, phone numbers, email addresses, credit card numbers, and other financial details may be included. Numerous factors, including cyberattacks, insider threats, and human mistake, can result in data breaches. A breach can cause identity theft, financial fraud, and other types of harm for customers. Supermarkets must put strong security measures in place, such as encryption, access controls, and monitoring systems, to prevent data

ISSN: 2582-6433

breaches. Additionally, they must constantly test their security systems to make sure they are working properly and teach their staff on how to recognise and stop data breaches.

If a breach happens, the impacted supermarket must notify its consumers right away and give them instructions on how to safeguard their personal data. To investigate the breach and stop such events from happening in the future, the supermarket should also collaborate with law enforcement and other pertinent authorities.

Two databases belonging to the US supermarket business Wegmans Food Markets were online and accessible because of a "misconfiguration." As a result, the business has disclosed a data breach. These databases purportedly held consumer information such as names, addresses, phone numbers, birth dates, Shoppers Club numbers, email addresses, and passwords for Wegmans.com accounts, according to the company with its headquarters in New York. Wegmans claims that account passwords were hashed and salted, and that neither financial nor social security information was accessed[1].

b) GADGET SERVICE CENTRE

Gadget service centres are entrusted with the responsibility of repairing and maintaining customers' electronic devices. While most service centres prioritize customer privacy and adhere to ethical practices, there have been instances where breaches of privacy have occurred.

A four-part study was carried out by researchers Jason Ceci, Jonah Stegman, and Hassan Khan to assess the level of privacy in the electronics repair sector. They started by asking 18 repair service providers—national (big-box stores), regional (stores of a larger chain), local (mom-and-pop shops), and device manufacturers—if they have a privacy policy or have put in place controls to protect the personal information of device owners from prying technicians. They discovered that the majority do not. During follow-up interviews with some of the respondents, it was also discovered that many service providers simply have a general policy on data collecting that fails to address crucial issues for the use case of (computer or smartphone) device maintenance and fails to include safeguards for

[1] US supermarket chain Wegmans suffers data breach due to 'misconfigured' databases | The Daily Swig (portswigger.net)

ISSN: 2582-6433

the data of clients[2].

The telecom giant's security failure is probably tied to Google's confirmation that Google Fi, its cellular network operator, also experienced a data breach. However, it is said that Google Fi largely uses US Cellular and T-Mobile's 5G networks. It is noteworthy that the tech giant omitted mentioning T-Mobile from the email[3].

c) E-COMMERCE

When customers register on e-commerce websites or make purchases, these corporations collect personal information about them. Name, address, phone number, email, and payment information are possible inclusions in this data. There have been cases where e-commerce businesses have improperly managed or misused consumers' personal information, resulting in violations of data privacy[4].

(a) Flipkart - After it was found that Flipkart was using its customers' personal information without their permission in 2020, the firm was charged with breaking data privacy rules. It was discovered that the corporation shared users' private information with its vendors, raising questions about the security of consumers' data.

(b) Amazon - After it was discovered that its Alexa voice assistant was secretly recording and storing customer chats without their permission, Amazon was charged with violating data privacy laws in 2018. Concerns were raised by the event over the security of user data and the possibility of data misuse.

(c) Paytm - After it was discovered that Paytm was disclosing users' personal information to third parties without their permission in 2018, the firm was charged for violating data privacy laws. Concerns were raised by the event over the safety of user data and the potential for information misuse.

These incidents not only increase the threats to a company's reputation, finances, and operations, but they also cost an organisation on average $3.86 million and take 280 days to contain. E-

Electronics repair technicians snoop on your data - Help Net Security
[3] T-Mobile hacking: Google Fi customers also hit by data breach - Times of India (indiatimes.com)
[4] Data Privacy Violation by E-commerce in India: Are Your Personal Information Safe? (linkedin.com)

ISSN: 2582-6433

commerce enterprises oversee a variety of financial and personal information that they must safeguard and keep safe from cyber criminals, including credit card information, customer addresses, and birthdates.

E-commerce businesses are additionally exposed to a wide range of additional cyber security threats, such as denial-of-service (DoS) assaults that can bring your website to a halt, automated bots that try to make purchases using stolen credit card numbers, and e-skimming assaults in which malware is installed on checkout pages to steal customers' personal information. Platforms for customer relationship management (CRM) and customer data management (CDM) in the cloud may provide a point of entry for hackers, particularly if these systems lack strong security standards or connect to networks with weak endpoint protection.

Hackers can easily get unauthorized access to your company's priceless customer data or confidential information if these applications—and the devices that hold them—do not use strong authentication or data encryption techniques[5].

d) TELECOMMUNICATION

Telecommunications companies are among the long-standing pillars of communication. From telephone infrastructure to internet service, they have helped businesses function and economies grow and whether it's for phone conversations or sending emails, people depend on telecoms every second of the day. Because of their increasing reliance on telecommunications and the sensitive data that passes via their networks, these businesses are particularly alluring to hackers. In 2019, DNS-based malware affected nearly 43% of telecom firms, and 81% of them reacted slowly by delaying the installation of the essential patches for the breach for up to three days[6].

TPG Telecom is added to the list of Australian companies that have been hacked. According to TPG, Australia's No. 2 internet service provider with 7.2 million members, the main objective of the hack of the hosted exchange firm was to hunt for client bitcoin and bank information. The intrusion was discovered by Mandiant, its cybersecurity advisor, during a forensic historical examination. TPG does

[5] The Economic Impact of Data Security Breaches in E-Commerce | Verizon Business
[6] 8 Telecom Industry Security Threats and How to Deal with Them - (q5id.com)

ISSN: 2582-6433

not provide figures on individual corporate accounts, but according to its 2021 annual report, corporate clients make for about 29% of its pre-tax profit. The company stated that every customer on the exchange service affected by the problem had been contacted and that precautions had been taken to prevent unauthorised access[7].

Vodafone data was leaked! information on 20 million clients and study by CyberX9 found that the loss of around 20.6 million people's private call records left Vodafone Idea customers exposed. The customer's full name and address, call location, call duration, SMS details, and other private information are among the sensitive data that was exposed in the Vodafone data breach. According to the inquiry, personal information, internet usage, and roaming usage data of post-paid Vi subscribers were also compromised. Himanshu Pathak, the founder and general manager of CyberX9, claims that the company emailed Vodafone Idea with all its results. Vi confirmed receiving our tip late on August 22, the individual said. Vodafone Idea has admitted to the security holes we discovered and brought to your attention on August 24[8].

e) APPS

Mobile apps have a significant impact on consumer data privacy, as they often collect large amount of personal data from users. This data can include information such as location, browsing history, contacts, and personal preferences. While some apps collect this data for legitimate reasons, such as improving the user experience or providing tailored advertising, others may use it for more nefarious goals, such as selling it to third-party advertisers or utilising it for identity theft.

Furthermore, many mobile apps need users to agree to lengthy privacy rules that may be difficult to read or involve legal language. This makes it difficult for users to understand what data is being gathered, how it is being used, and with whom it is being shared. To preserve customer data privacy, many nations have enacted rules and regulations requiring mobile app developers to be upfront about their data gathering and usage practises. For example, the European Union's General Data Protection Regulation (GDPR) requires organisations to seek explicit agreement from users before collecting

[7] TPG Telecom joins list of hacked Australian companies, shares slide, ET Telecom (indiatimes.com)
[8] Vodafone data leaked! 20 million customers information hacked, says CyberX9; Vi reacts | Tech News (hindustantimes.com)

ISSN: 2582-6433

personal data.

(a) There are some health-related apps which may sometimes breach the consumer privacy by selling it to the 3rd parties. And we are living in a golden era of healthcare innovation. The health tech market is predicted to increase at a 15% annual rate and quadruple in value to US$300 billion by 2028 (up from US$110 billion now). The digital health market has expanded by 12% in the last year, owing to the covid-19 epidemic, which has created a surge in demand for telehealth solutions. Telehealth isn't the only growing industry. mHealth apps are utilised by billions of people worldwide, with over 350,000 mHealth apps presently available in major app stores. "mHealth" refers to a wide range of smartphone apps or wearable devices that allow consumers to track and monitor everything from exercise and nutrition to menstruation and sleep habits, as well as allowing professionals to communicate, monitor, and diagnose patients more quickly and accurately[9].

(i) The Optus Macquarie University Cyber Security Hub in Sydney recently conducted a study on more than 20,000 mobile health apps available on the Google Play Store from Australia and around the world and found that the vast majority of mHealth apps contain serious privacy issues — 88% of these apps included code that can access and share users' personal data with third parties; roughly 28% of apps did not even have a privacy policy; and apps were frequently updated.

(ii) For sharing patient personal information with private health insurance brokers, Health Engine, an Australian patient booking platform and online health care directory that lists over 70,000 medical practises and practitioners, was fined over $3 million by the Federal Court in 2020.

(iii) As was the case with free apps marketed to people with depression or who want to quit smoking, which are reportedly haemorrhaging user data to third parties like Facebook and Google but often don't admit it in their privacy policies, nearly all of the apps gave third parties, including Facebook and Google, access to user data. This is true even of apps that claim to be for treating opioid addiction.

(iv) A Wall Street Journal investigation revealed that period monitoring software Flo shared users' cycle dates and potential pregnancies with Facebook.

(v) 2019 saw the discovery that the app for comparing the cost of prescription drugs User data was being shared by GoodRx with marketing companies like Facebook and Google.

[9] Why mHealth apps are bad at privacy, and what they can do about it (linkedin.com)

ISSN: 2582-6433

(b) Retailer apps have become increasingly popular as more consumers turn to mobile devices for shopping. However, these apps can pose a risk to consumer data privacy if they are not properly secured and protected. Sensitive consumer data, including names, addresses, phone numbers, email addresses, and credit card information, may become public if a shop app has a data breach. Retailer apps can make purchasing more convenient and simpler for customers, but they also carry a danger to data privacy if the right security steps aren't taken. Retailers must take the appropriate precautions to safeguard the personal information of their customers, and customers must be diligent in securing their own information.

These instances demonstrate how even well-established, financially savvy businesses may fail to adequately protect their consumers' privacy and security when using mobile apps[10].

(i) Under Armour's market value decreased by 3.8% because of a vulnerability in the MyFitnessPal mobile app that allowed threat actors to gather the personal information of more than 150 million users.

(ii) A security flaw in a mobile app at British Airways resulted in the exposure of 380,000 credit card purchases and the vulnerability of private user information. The incident significantly reduced market value and eroded consumer confidence.

(iii) After an investigation revealed that mobile app vulnerabilities exposed sensitive client information, Equifax, Western Union, and three other financial service organisations suffered damage to their reputations. Each corporation was required to improve mobile app security as part of a deal with the New York Attorney General's Office.

f) CYBER-ATTACK

A cyber-attack can have a significant impact on consumer privacy, as it can result in the theft or exposure of personal information. Cyber-attacks can take many forms, including hacking, malware, phishing, and ransomware, and they can target individuals, businesses, or even government agencies. When personal information is stolen or exposed in a cyber-attack, it can be used for identity theft, fraud, and other malicious purposes. This can include opening new credit accounts in the victim's name, making unauthorized purchases, or even committing crimes using the victim's identity.

[10] How Privacy Issues in Mobile Apps Impact Retailers - Retail TouchPoints

ISSN: 2582-6433

(a) Here have been many major data breaches caused by cyber-attacks in the 21st century. Some notable examples include[11],

(i) Yahoo claimed the updated estimate did not indicate a new security issue and stated it was sending emails to all additional affected user accounts. Yahoo, which experienced a distinct attack from the one previously mentioned in 2013, is making its second appearance on this list. Initial corrective action was taken by the corporation in 2014, but it wasn't until a stolen database was sold on the black market in 2016 that Yahoo made the information public.

(ii) Aadhaar is linked to Alibaba - The world's largest ID database, Aadhaar, was breached by malicious actors in the early months of 2018, revealing information on more than 1. 1 billion Indian individuals, including names, addresses, phone numbers, emails, and biometric information like fingerprint and iris scans.

(iii) LinkedIn - Although LinkedIn asserted that the incident was not a data breach because no sensitive, private personal data was disclosed, a sample of the scraped data posted by God User contained information such as email addresses, phone numbers, geolocation records, genders, and other social media specifics, which would provide criminals with plenty of data to produce convincing, follow-up social engineering attacks after the leak, as warned by security experts.

(iv) Facebook - Given the sheer volume of phone numbers affected and made readily available on the dark web as a result of the incident, Troy Hunt, a security researcher, actually added functionality to his HaveIBeenPwned (HIBP) breached credential checking site that would allow users to check if their phone numbers had been included in the exposed dataset.

(v) Given the sensitive nature of the services offered by the company, which includes casual hook-up and adult content websites like Adult Friend Finder, Penthouse, the breach of more than 414 million accounts names, email addresses, and passwords had the potential to be particularly devastating for victims.

[11] The 15 biggest data breaches of the 21st century | CSO Online

ISSN: 2582-6433

(b) The SolarWinds breach which affected several government agencies and other recent cyberattacks like the one on Colonial Pipeline Co. have exposed serious flaws in critical infrastructure systems and government cybersecurity protocols, necessitating immediate action from the White House. If these breaches have taught us anything, it's that organisations of all sizes and in all sectors need to take every precaution to safeguard their networks, environments, and equipment. Whether its employee remote access to internal systems or access given to third-party contractors who handle outsourced business processes, organisations deal with risks to their environments every day. There are plenty of opportunities for hackers to take advantage of, particularly for significant and vulnerable targets like the government and key infrastructure[12].

3) PROBLEM FACED DUE TO BREACH OF PRIVACY

Any retail or e-commerce organisation that experiences a data breach may face serious financial, reputational, and legal repercussions. However, these frequently take a backseat to the consequences for customers whose personal data was taken in terms of money, career, emotions, physical health, and mental health. About 15,000 people seek assistance from the Identity Theft Resource Centre each year to deal with the debilitating repercussions that a data breach has had on their daily life. And financial worries are just the start of a horrific litany of potential effects when a customer's data is stolen, according to the ITRC's 2022 Consumer Impact Report. A new victim is reported every 22 seconds in the United States, as per National Council on Identity Theft Protection, and there are roughly three times as many cases here than abroad. That amounts to an enormous 1.5 million victims annually[13].

i) Mental health damage – Being a victim of a data breach can cause emotional distress and anxiety. The invasion of privacy, loss of control over personal information, and uncertainty about the extent of the breach's impact can take a toll on consumers' mental well-being.

[12] Cyberattacks reveal the truth about network vulnerability | Imprivata
[13] What Happens to a Customer After a Data Breach? - Security Boulevard

ISSN: 2582-6433

Recent unpublished records revealed that a sizable number of instances where psychological disputes following a data breach were discovered showed a level of disturbance and disruption consistent with a recognised psychological disorder, such as adjustment disorders, depressive disorders, generalised anxiety disorders, and in the worst cases, PTSD. All parties are better able to rationally comprehend the severity of an issue and whether treatment is necessary to address it after a proper diagnosis has been made. It's less probable that a data breach would satisfy the requirements of a life-threatening incident (with possible PTSD ramifications). However, the 'knock on' impact of a significant data breach might theoretically lead to high levels of stress and following unfortunate life occurrences with significant repercussions[14].

ii) Financial loss – Data breaches can lead to financial losses for consumers. If cybercriminals gain access to banking or credit card information, they can make unauthorized transactions, drain bank accounts, or use credit cards fraudulently. Consumers may be left dealing with the aftermath of fraudulent charges, having to resolve discrepancies with financial institutions, and potentially losing money.

A data breach would typically cost $4.24 million on average in 2021, up from $3.86 million on average in 2019, according to the most recent data breach report from IBM and the Ponemon Institute. What's more alarming is the report's conclusion that the greater a breach's financial impact, the longer it goes unnoticed[15].

iii) Loss of privacy and trust - Consumers' trust in the companies tasked with protecting their data is damaged by data breaches. This decline in confidence may limit their desire to use digital services or provide private information, which would negatively influence their whole online experience.

When a data breach occurs, customers lose trust in the business. They begin to wonder if they should keep doing business with the corporation considering this. They might no longer have any faith in the firm and decide to shop around.

[14] https://www.hughkochassociates.co.uk/article/do-data-breaches-cause-stress/
[15] The Consequences of a Cyber Security Breach (sungardas.com)

ISSN: 2582-6433

The consequences of this decline in client confidence may be long-lasting. A consumer won't use your services again if they decide not to. You'll lose out on possible income. You must have a backup strategy as a company to limit the harm that a data breach can do[16].

iv) Identity theft – Personal identifiable information (PII) like names, addresses, Social Security numbers, and dates of birth is frequently exposed in data breaches. This information can be used to perform identity theft, in which criminals exploit victims' identities to start fictitious accounts, apply for loans, or carry out other illicit acts. The impacted consumers may have financial and legal issues as a result. When e-commerce companies manage customers' personal information poorly, they put them at danger of identity theft. Identity theft is the practise of taking someone else's personal information and using it for fraudulent or other illegal purposes[17].

4) LAWS DEALING WITH CONSUMER DATA BREACH

4.1 INDIA

i) According to the Consumer Protection Act of 2019, section 2(47)(IX), which was in effect at the time, it is illegal to expose to a third party any personally identifiable information provided in confidence by the customer unless obligated to do so by law[18].

ii) The Indian Constitution does not clearly guarantee the basic right to privacy. The courts have incorporated the right to privacy among other fundamental freedoms previously recognised by the Indian Constitution, including the freedom of speech and expression under Article 19(1)(a) and with the Article 21 right to life and personal freedom. However, the State may impose the reasonable restrictions outlined in Article 19(2) of the Constitution, which apply to these Fundamental Rights under the Indian Constitution[19]. In the landmark decision of Justice K S Puttaswamy (Retd.) vs. Union

[16] How Does a Data Breach Affect Your Customers? (primeview.co)
[17] Data Privacy Violation by E-commerce in India: Are Your Personal Information Safe? (linkedin.com)
[18] https://egazette.nic.in/WriteReadData/2019/210422.pdf
[19] Data Protection Laws In India - Everything You Must Know - Data Protection - India (mondaq.com)

ISSN: 2582-6433

of India and Ors., the constitution bench of the Hon'ble Supreme Court recently held that the right to privacy is a basic right, subject to some understandable limitations[20].

iii) The (Indian) Information Technology Act, 2000 addresses concerns related to civil and criminal penalties for improper disclosure, misuse, and breach of contract involving personal data[21].

As per this act some section deals with penalization of offence of data breach[22]

(1) In accordance with section 43A of the (Indian) Information Technology Act, 2000, a body corporate that is in charge of, dealing with, or handling any sensitive personal data or information and is negligent in establishing and maintaining reasonable security practises that cause wrongful loss or wrongful gain to any person may be held liable to pay damages to the person so affected. It's important to highlight that in certain situations, the impacted party's request for compensation has no upper limit.

(2) Information disclosure made knowingly and wilfully without the person's consent and in violation of a valid contract is prohibited under section 72A of the (Indian) Information Technology Act, 2000, and is subject to up to three years in jail and a fine of Rs 5,00,000 (about $8,00).

(3) According to a residual provision in Section 45 of the IT Act, anyone who violates any rules made under the IT Act for which no specific penalty has been imposed is subject to compensation or a penalty of up to 25,000 rupees. Section 45 applies to all parties, including people and organisations as well as employers and workers.

(4) According to the Information Technology (Amendment) Act of 2008, anyone who enters a computer without permission, makes an unauthorised digital copy, downloads, or extracts data, violates someone's privacy, etc., is subject to civil liability for computer database theft. A person is also responsible for paying damages as restitution for a variety of cybercrimes, according to Section 43.

[20] https://indiankanoon.org/doc/127517806/
[21] Data Protection Laws In India - Everything You Must Know - Data Protection - India (mondaq.com)
[22] All about data privacy breach in India - iPleaders

ISSN: 2582-6433

4.2 EUROPE

The General Data Protection Regulation (GDPR) governs the privacy and protection of personal health data in Europe. The GDPR, which is currently regarded as the industry benchmark for data protection, sets rigorous criteria for the collection, storage, and use of personally identifiable information (PII), which broadly speaking encompasses any type of medical or personal information that may be gathered by mHealth apps. Among other things, the GDPR mandates data protection, data minimization, and privacy by design and default[23].

Any data breach that poses a danger to the privacy of people impacted must be reported to data protection regulators, as required by the GDPR, as well as any affected persons. Notifying the public considerably raises the expenses of reacting to a data breach and the likelihood that those impacted will file lawsuits against the controller[24].

The General Data Protection Regulation, or GDPR, became operative in the EU in May 2018. The law's ability to be enforced has substantial effects. The maximum fine for a violation is 20 million Euros, or 4% of the company's global annual revenue, whichever is higher. The General Data Protection Regulation (GDPR) infractions in 2020 resulted in fines of $193 million (€159 million) from European data agencies, with the biggest sanction of $57 million levied against Google by French authorities[25].

4.3 CALIFORNIA

The CCPA improves a person's access to and security of their personal data. These rights include the opportunity for a person to object to processing, the right to have their data erased, and the right to have their data portable—in an electronic format. This suggests that a policyholder may request a copy of all the data that their current insurer has on them in a commonly used and machine-readable format so they can provide it to their new insurer. Any automated decision-making processes must be disclosed in the privacy notice that the insurer provides. Individuals will be entitled to object to

[23] Why mHealth apps are bad at privacy, and what they can do about it (linkedin.com)
[24] Cybersecurity and Data Privacy | AmTrust Insurance (amtrustfinancial.com)
[25] The Consequences of a Cyber Security Breach (sungardas.com)

ISSN: 2582-6433

automated decision-making as well, thus the insurer will need to offer a non-automated alternative[26]. The California law also imposes penalties on businesses that fail to comply with its standards. In the event of a consumer action for data breaches or data theft where there was insufficient data protection, the fines range from $100 to 750 (or the cost of real damages, whichever is more) per residence and occurrence.

In the case that the State Attorney General files a lawsuit, the penalties range from $2,500 for an unintentional infraction to up to $7,500 for a wilful one. When minors are harmed intentionally or unintentionally, the maximum penalties are $7,500. The CPRA does not allow businesses a 30-day window to fix violations after being informed of them, in contrast to the CCPA[27].

4.4 SWITZERLAND

When a person's data is handled, the Federal Act on Data Protection (FADP) attempts to safeguard that person's right to privacy as well as their other fundamental rights. In 1992, when the FADP was established, neither the Internet nor the digital world of today had yet seen widespread commercial use. The updated FADP will go into effect on September 1, 2023. It will contain adjustments aimed at better protecting the private information of Swiss individuals. Companies must, for instance, explain why they gather customer information and disclose which other parties with whom they share it. People will also have a right to information about the duration of data storage and the uses to which it will be put. Inaccurate data may also be requested to be corrected, and they are not needed to provide a justification [28].

The FADP incorporates "privacy by design" and "privacy by default" principles into the law. This necessitates that businesses consider data processing principles during the development and design phases of applications rather than focusing only on data security and protection in the after-the-fact stage. Furthermore, they are prohibited from obtaining the agreement of data subjects for any

[26] Cybersecurity and Data Privacy | AmTrust Insurance (amtrustfinancial.com)
[27] 11 new privacy laws around the world and how they'll affect your analytics - Piwik PRO
[28] https://www.adnovum.com/blog/swiss-federal-act-on-data-protection-2023#:~:text=The%20Federal%20Act%20on%20Data%20Protection%20(FADP)%20aims%20to%20protect,reality%20was%20not%20yet%20foreseeable.

ISSN: 2582-6433

processing that is not strictly necessary by using web technologies' default settings, for example.[29]

4.5 CHINA

China enacted the PIPL, or Personal Information Protection Law. The Data Security Law (DSL) and Cybersecurity Law (CSL) were two previous data security laws that were in effect before the Personal Information Protection Law (PIPL), but the PIPL is the first complete law created in China to govern and protect personal information. China's data security and privacy rules are now considerably more in line with global standards thanks to the implementation of DSL and PIPL. Numerous PIPL components are strikingly like GDPR. Even if you've already complied with GDPR regulations, it won't be difficult to adapt to PIPL if you undertake some gap analysis between GDPR and PIPL standards. [30]

Penalties might be as much as 5% of the income from the preceding year, or 50 million yuan (about $7.7 million). Fines ranging from 100,000 to 1,000,000 yuan are imposed on directly accountable personnel. Personal information protection authorities may issue a rectification order, give warnings, and seize any illegal proceeds if the processing of personal information violates the PIPL's provisions. A punishment of up to RMB 1,000,000 (about USD 145,204.00) may be imposed on those who refuse to make the necessary corrections. A punishment of between RMB 10,000 (about USD 1,452.00) and RMB 100,000 (about USD 14,520.00) shall be imposed on the person in charge and those staff members who are directly responsible.[31]

A person commits a crime, in accordance with the Ninth Amendment to the Criminal Law, if they (a) gain Personal Information (PI) belonging to Chinese nationals by illegal methods, or (b) sell or distribute PI belonging to Chinese people to third parties "contrary to relevant statutory provisions". Offenders who commit "serious" offences may get a fine and a three-year maximum sentence. Offenders may get a maximum seven-year jail term in "particularly serious" circumstances.[32]

[29] https://usercentrics.com/knowledge-hub/switzerland-federal-data-protection-act-fadp/
[30] 11 new privacy laws around the world and how they'll affect your analytics - Piwik PRO
[31] https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/china/topics/penalties-for-non-compliance#:~:text=If%20the%20processing%20of%20personal,USD%20145%2C204.00).
[32] https://www.bclplaw.com/en-US/events-insights-news/part-4-of-5-penalties-and-liabilities-under-chinas-data-protection-laws.html

ISSN: 2582-6433

5) SOULTIONS CAN BE MADE

To help prevent data breaches and protect consumer data, here are some solutions and best practices that individuals and organizations can adopt:

a) **Strong and Unique Passwords**: Use strong, complex passwords for online accounts and avoid reusing passwords across multiple platforms. Consider using a reputable password manager to generate and store your passwords securely.

It is true that "password123" is no longer an effective security measure (although I'm not convinced it ever truly was). Make it a point to use a combination of capitalization, symbols, and alphabetic and numeric characters while creating clever passwords. Better, use encryption to provide an extra degree of security. Purchase a password-management programme like LassPass. To securely save your credentials and make sure that they can't be read in the case of a cyberattack, these solutions employ encryption.[33]

b) **Two-Factor Authentication (2FA):** Enable 2FA whenever possible, as it adds an extra layer of security by requiring a second form of verification, such as a code sent to your mobile device, in addition to your password. It combines everything that you have, like as your fingerprints or another biometric, with everything that you know, such as your password and login, as well as everything that you own, such as a mobile device or a physical security key. Two-factor authentication is the name of this procedure, also referred to as "two-step verification." This procedure checks if a user is authorised to log in. Using methods like "credential stuffing," "password spraying," or brute-force attacks, hackers may find it simple to get access to and take control of several people' internet accounts. This happens often. Even IT giants like Cisco and Apple's iCloud service, as well as cellular networks, retail behemoths, food delivery services, music streaming websites, and other industries, are not immune.[34]

c) **Be Cautious of Phishing Attempts**: Be vigilant about suspicious emails, messages, or calls requesting personal information. Do not open attachments or click on links from unverified or

[33] https://blog.hubspot.com/service/protecting-customer-data#how-to
[34] https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/

ISSN: 2582-6433

suspicious sources. Verify the legitimacy of communications before sharing any sensitive information.

Due to spam screening, many scam emails might not reach your mailbox. However, spam filters are frequently defeated by scammers, so it could be advantageous to add more layers of security. Here are four ways to protect yourself from phishing frauds. Use security software to ensure that your machine is protected. To protect your mobile device, set software to update automatically. You may safeguard your accounts by using multi-factor authentication. To protect your data, create a backup.[35]

d) **Regularly Update Software and Devices**: Keep your operating systems, apps, and devices up to date with the latest security patches These updates frequently contain crucial security patches that can aid in preventing known vulnerabilities. Even well used and trusted software can contain bugs. The best app development companies keep an eye out for them and take them down as soon as they are found.

You might keep your phone safe and your data protected by doing a quick programme update. It is your responsibility to regularly update your applications to fix any faults that may have mistakenly crept into your code and maintain the functionality of your apps. Another wise choice is to get rid of unwanted programmes. Even if you aren't using an application, keeping it on your phone makes sense for storage and privacy reasons.[36]

Cyber assaults frequently occur because of gaps in your software or system updates that create security vulnerabilities. Cybercriminals thus take advantage of these flaws to infiltrate your network. Taking preventive measures is frequently impossible after they have entered.[37]

e) **Avoid using public Wi-Fi:** You also expose yourself to a multitude of risks when you use apps on your mobile device over a public network. If you have some spare time to spend and are at an airport or café with free Wi-Fi, it's likely that you will pick up your phone and open one of the apps. However, there are many attackers and harmful programmes that live on public Wi-Fi. This does not imply that

[35] https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#protect
[36] How to Protect Your Data Privacy on Mobile Apps (moveoapps.com)
[37] https://leaf-it.com/10-ways-prevent-cyber-attacks/

ISSN: 2582-6433

you never utilise free Wi-Fi. Simply said, it only shows that you are selective about what you do and don't do when using a public Wi-Fi network. Go ahead and look up some of your favourite coffee table designs or the most recent headlines. However, you might want to hold off on placing an order for groceries or a new pair of shoes until you arrive at your destination. Using shopping applications on a public Wi-Fi network is not a good idea since they have access to your credit card information.[38]

f) **Antivirus programme:** Ensure that your server is regularly safeguarded and supervised by installing current antivirus, antispyware, and anti-malware software. Such software shields data assets from theft or destruction by hostile malware such as your mobile phone or pc.[39]

6) CONCLUSION

Because it prevents unauthorised access to, use of, or publishing of their personal information, such as name, address, phone number, and financial information, consumers appreciate data privacy. There are several ways that data from various platforms, such as shops, telephones, apps, and e-commerce websites, might be hacked. The consumer also must cope with several major consequences because of the companies' negligence in preserving the data, which has a detrimental effect on both their mental health and their financial status. The overall lack of care and laziness of customers makes this situation worse. India is one of several nations that have laws in place to safeguard consumer privacy and provide severe fines in the case of a violation. Customers may take security measures to protect themselves by utilising two-factor authentication, creating strong passwords, avoiding risky public Wi-Fi, and staying current with software updates.

[38] How to Protect Your Data Privacy on Mobile Apps (moveoapps.com)
[39] https://www.lepide.com/blog/ten-ways-to-prevent-network-security-breaches-in-the-workplace/