ISSN (O): 2349-8293

STUDENT LAW REVIEW

RAJIV GANDHI NATIONAL UNIVERSITY OF LAW STUDENT LAW REVIEW

VOLUME 7 2021 ISSUE 1

THEME:

"PROTECTING CONSUMERS IN THE 21ST CENTURY: BROADENING THE OUTLOOK"

RGNUL STUDENT RESEARCH REVIEW

Formerly

RGNUL Student Law Review (RSLR)

ISSN: 2349-8293 (Online)

Website: **www.rsrr.in**

Published by:

The Registrar

Rajiv Gandhi National University of Law

Sidhuwal - Bhadson Road

Patiala – 147001

Punjab, India

www.rgnul.ac.in

Cite this Volume as:

7(1) RSRR <Page Number> (2021)

RGNUL STUDENT RESEARCH REVIEW

Formerly

RGNUL Student Law Review (RSLR)

RAJIV GANDHI NATIONAL UNIVERSITY OF LAW, PUNJAB

VOLUME 7

ISSUE 1

THEME:

"PROTECTING CONSUMERS IN THE 21ST CENTURY: BROADENING THE OUTLOOK"

2021

PEER REVIEW BOARD

BOARD OF EDITORS

ABOUT THE COLLABORATOR

Saikrishna & Associates is a Tier-1 full-service Firm with Intellectual Property, Telecommunication Media & Technology, Corporate Law & Competition Law verticals backing up the Firm's other practice areas.

Founded in 2001, the Firm's 19 Partners and Associate Partners as well as 100+ lawyers deliver top-notch and dedicated services to a diverse array of Indian and International clients. The industry teams and practice groups span across the sectors of media and entertainment, telecommunications and electronics, pharma and life sciences, software and artificial intelligence, automotive, FMCG and retail, print-publishing, real estate, and energy.

The Firm's commitment to excellence and diligence allows it to count some of the biggest companies, internationally as well as in India, as its long-standing clients. The Firm's Litigation/ Dispute Resolution, Prosecution, and Enforcement teams join with the Commercial, IP, TMT, Corporate and Competition law teams to provide innovative solutions catering to client's business and IP objectives.

The Firm is highly ranked for their industry and domain-specific expertise. The Firm now is now diversifying into academia.

AIM OF THE JOURNAL

Consumption is the sole end and purpose of all production; and the interest of the producer ought to be attended to, only so far as it may be necessary for promoting that of the consumer.

-Adam Smith

In 2020, Justice A.M. Khanwilkar highlighted the phrase "*Consumer is the king*",[1] which underscores the importance of the consumers' interest. Consumer trust and confidence are the hallmarks of a robust consumer protection mechanism, which forms the foundation of a sound market system.[2] The advancement of consumer rights requires negation of information asymmetry and unethical business practices, an objective which must guide the future development of consumer laws.

Consumer rights and consumerism have gradually gained importance. Historically, the onus of judging a product's quality rested on the buyer.[3] Even though ancient texts like Manusmriti emphasized ethical trade practices,[4] the principle of caveat emptor (let the buyer beware) prevailed. Eventually, it was realized that reasonable examination by a consumer cannot reveal the inherent defects, especially in complex products,[5] the knowledge of which is possessed only by the seller. Thus, arose the need for protecting the consumer; and the responsibility was shifted, to some extent, on the seller, laying the foundations of *caveat venditor* (let the seller beware).

In India, certain legislations such as the Indian Penal Code, 1860, the Sale of Goods Act, 1930, the Essential Commodities Act, 1955, the Prevention of Food Adulteration Act, 1954, the Drugs and Cosmetics Act, 1940, among others, constituted the legal framework that catered to consumer protection. Most notably, the provisions of the Sale of Goods Act marked a perceptible shift to *caveat venditor* by introducing the concept of merchantable quality, seller's skill and judgment.[6] Consumer rights were formally recognized in India with the Consumer Protection Act, 1986 ("**CPA 1986**").

The CPA 1986 was a welcome step. It established a holistic structure of grievance-redressal mechanisms and emboldened the consumer through

[1] Branch Manager, Indigo Airlines v. Kalpana Rani, (2020) 9 SCC 424.
[2] Chapter-1, Manual on Consumer Protection, 2016, UNCTAD, https://unctad.org/en/PublicationsLibrary/webditcclp2016d1.pdf, last seen on 12/08/2020.
[3] Whitmore v. Orono Pulp & Paper Co., 39 A. 1032, 1036 (Me. 1898).
[4] Manusmriti, Chapter X, verse 115, https://www.sacred-texts.com/hin/manu/manu10.htm, last seen on 12/08/2020.
[5] Chapter-9, Manual on Consumer Protection, 2016, UNCTAD, https://unctad.org/en/PublicationsLibrary/webditcclp2016d1.pdf, last seen on 22/08/2020.
[6] S. 16, the Sale of Goods Act, 1930.

the introduction of remedies against unfair or restrictive trade practices, hazardous goods, and defective goods inter alia. To spread awareness regarding consumer rights and educate the consumers against prevailing malpractices of the sellers, the Indian Government's launched its noteworthy consumer awareness campaign, "*Jago Grahak Jago*" back in 2005. To adapt to the digital age, the campaign is now being revamped to spread awareness through social media platforms.

The dawn of the 21st century has witnessed drastic changes in the market dynamics, the modus operandi of businesses and the technological landscape.[7] It has become tough to attribute liability for deficiency in services due to the multiplicity of entities involved in modern-day transactions. To combat new challenges, improved regulatory measures were needed. India drew inspiration from consumer protection legislations in countries like the US, Singapore, France, etc., and from the European Union Directives, and passed the Consumer Protection Act, 2019 ("**CPA 2019" / "the Act**") (enforced in 2020[8]). This Act replaced the 33-year-old CPA 1986.

The CPA 2019 has introduced new concepts to protect the consumer, namely criminal liability,[9] product liability,[10] liability for misleading/ false advertisements,[11] mediation for consumer disputes[12] and rules on e-commerce[13]. Provisions for liabilities vis-à-vis consumer protection were spread across different legislations; however, the CPA 2019 has consolidated many of those liabilities for simplification and creation of efficient enforcement machinery. Though criminal as well as product liability have been introduced, it is to be seen whether they act as a roadblock in the ease of doing business, and whether the age of Artificial Intelligence and Robots can be effectively regulated.

Structurally, the CPA 2019 has established a regulatory body in the form of the Central Consumer Protection Authority ("**CCPA**") and has increased the pecuniary jurisdiction of the District, State and National Consumer Protection forums. The CCPA is a centralized structure, introduced for supervision of the tiered consumer protection forums. The measure is perceived to aim at enhancing protection of consumer rights.

---

[7] The Consumer Protection Bill, 2019, Statement of Objects and Reasons, https://www.livelaw.in/pdf_upload/pdf_upload-362684.pdf, last seen on 12/08/2020.
[8] Ministry of Consumer Affairs, Food and Public Distribution, Notification S.O. 2351(E), https://consumeraffairs.nic.in/sites/default/files/Act%20into%20force.pdf, last seen on 22/08/2020.
[9] Chapter VII, The Consumer Protection Act, 2019.
[10] Chapter VI, The Consumer Protection Act, 2019.
[11] S. 89, The Consumer Protection Act, 2019.
[12] Chapter V, The Consumer Protection Act, 2019; The Consumer Protection (Mediation) Regulations, 2020.
[13] The Consumer Protection (E-Commerce) Rules, 2020.

According to the National Consumer Disputes Redressal Commission, over 4.8 lakh consumer cases are pending in the country.[14] The introduction of mediation, as an out-of-court-settlement, is a step in the right direction to allow speedy justice. However, questions as to the application of arbitration procedures or the Online Dispute Resolution ("**ODR**") methods for consumer disputes are yet to be resolved.

During the COVID-19 pandemic, instances of misinformation, disinformation and fake news have proliferated. In light of this, the timely introduction of liability for misleading advertisements is an essential safeguard for consumers. Despite these advances, issues like targeted advertisements, unsolicited commercial communications, among others, are likely to outstrip the reach of the existing provisions and impede the realization of their aims.

The definition of terms like 'consumer', 'service', 'deficiency', etc., has been widened; while certain other terms have been added in the CPA, 2019 to make it a holistic legislation. This has increased the ambit for regulation of unethical and restrictive trade practices. However, the Act covers only those services where consideration is involved. This places free public services beyond the scope of the Act, even though such services might pose considerable risks for unsuspecting consumers.

Since 2013, the number of consumer complaints received at the National Consumer Helpline has been exponentially increasing every year.[15] While the E-commerce rules have set the stage for consumer protection in this digital era, numerous concerns yet stand unaddressed; and this may potentially jeopardize the success of regulatory measures. *Can the existing regulatory framework manage to meet the ever-increasing challenges of the Digital Age?* The question warrants immediate attention.

Consumer protection is not a law that acts in a vacuum; rather, its realization and enforcement extend into several fields like environmental law, antitrust laws, intellectual property laws, privacy issues, amongst others. The theme of the World Consumer Rights Day, 2020, "*Sustainable Consumer*",[16] indicates the importance of global sustainable consumption and stands as a testament to the interdisciplinary nature of consumer law.

The provisions against tying and bundling of services in competition laws, or fair use of copyrights and licensing of patents under the IPR laws are

---

[14] Statistics, National Consumer Disputes Redressal Commission, http://ncdrc.nic.in/stats.html, last seen on 24/08/2020.

[15] Cheating by E-commerce Companies, Unstarred Questions No. 384, Ministry of Consumer Affairs, Food and Public Distribution, Department of Consumer Affairs, https://164.100.158.235/question/annex/246/Au384.pdf, last seen on 24/08/2020.

[16] The Sustainable Consumer – World Consumer Rights Day 2020 theme, Consumers International, https://www.consumersinternational.org/news-resources/news/releases/the-sustainable-consumer-world-consumer-rights-day-2020-theme/, last seen on 22/08/2020.

certain provisions that indirectly ensure consumer protection. However, there are several anti-competitive practices adopted by different entities which threaten the consumers by disrupting the market system; and thus, there arises a need to take another look at the existing antitrust laws from a consumer's perspective. In a globalized environment connected via digital means, IPR and consumer welfare has become more pertinent than ever.

Moreover, the interplay of the financial sector regulations and consumer protection laws is inevitable, particularly due to the rapid transition to a digital economy. The growing complexity of the transactions involved puts the consumers at risk of exploitation. The entry of FinTech and e-insurance mechanisms creates an entirely new environment for a consumer and their viability needs to be tested. The position of gig workers, prevalent in different sectors like the automobile industry or the food delivery aggregators, needs to be analyzed to assess whether they should be treated as consumers to protect their interest. The rising cases of insolvencies also ring alarm bells for a consumer as money invested in big conglomerates and companies might just be lost on account of an insolvency, whether it be voluntary or involuntary. *Should a consumer be treated as just another creditor? Should consumer redressal proceedings be allowed despite moratorium on other proceedings?*

Besides legislations at the domestic level, there are certain standards and principles adopted at the international level which include the UN Guidelines on Consumer Protection, 2015; Model UNCTAD Manual on Consumer Protection, 2017, among other guidelines. Moreover, there are certain multilateral organizations like the International Consumer Protection Enforcement Network and the ASEAN Committee on Consumer Protection that work at the international level and aim to establish cooperation between nations for consumer protection. However, despite the aforementioned endeavors, standardization and uniformity is yet to be achieved at the international level, especially where cross-jurisdictional issues arise.[17]

The recent turn of legislative measures has greatly emboldened the consumer in tackling the new challenges. However, despite adoption of the best practices from different jurisdictions, implementation and realization of the objectives of CPA, 2019 is yet to be tested. *Has the balance been tilted a bit too much in favor of the consumer? Are the existing interpretations and definitions enough to deal with the growing challenges or do they need a fresher outlook? Should a comparative approach be used to mold the present law?* The important question that stands in limbo is- *whether consumers in the 21st century are adequately equipped and informed to protect themselves?*

[17] M. Durovic, International Consumer Law: What is it all About?, 43 Journal of Consumer Policy, 125, 133, 2020.

While coursing through a plethora of incumbent issues in consumer protection, there arise questions both perennial and contemporary. In spite of considerable changes in laws aiming to adapt to the new developments, a strong consumer protection framework and an efficient consumer disputes redressal mechanism has always been a challenge for India.

In light of the changing market dynamics and evolving consumer protection laws, RSRR delves into the theme of "**Protecting Consumers in the 21st Century: Broadening the Outlook**", to review the legal and policy framework in today's consumer centric economy.

FOREWORD

Dear discerning reader,

"*Consumer is King and the King Never Bargains*" is a slogan that Indians have seen displayed in retail shops all over the country. This simple sentence brings forth a concern: does the modern-day consumer have the power to bargain? With price tags and effective competition governing the pressure on consumer's pockets, further research on consumer protection methods from a legal perspective becomes imperative. In actual fact, changes in different legislations are bound to have an impact on the consumer. Alterations or additions to competition policies, food regulation, corporate liability and even intellectual property rights tend to influence consumer choices and benefit.

The need to do away with the old consumer legislation and draft one afresh was reflected in the culmination of the Consumer Protection Act, 2019 ("**the Act**") which came into effect in July 2020. Not only has the ambit of the Act increased to include e-commerce portals, but contradictory precedents have continued to redefine the horizon of the services that fall within the ambit of the consumer legislation. The *prima facie* intent is to forge a safe path for the consumers concerned. Healthcare services, specifically when free,[1] and education, have often faced test of 'service' under the legislation.

The Product Liability framework introduced within the Act has enticed the interest of the legal fraternity. Probing into the viability of this framework would highlight issues such as unnecessary additional costs[2] and the extent of the liability so imposed on the people involved in the supply chain. It has to be meticulously deliberated whether imposition of criminal penalties on body corporates will be effective vis-a-vis heavier monetary penalties on the body corporations. Another concern that comes to the forefront is that an employer may escape conviction by putting the blame on an employee.[3]

The pandemic and lockdown measures have gravely altered consumer behavior, with demands now being met via online platforms. Global shopping sites have further diminished borders. The E-commerce-Big Data duo has been spiraling multiple dialogues ranging from 'harm' in relation to the personal data of consumers to influencing consumers through 'dark patterns'. From targeted advertisements to top-grade customized services, consumers have been put under the spotlight. Is

[1] Union of India v. N.K. Srivastava, 2020 SCC OnLine SC 636.
[2] A.M. Polinsky & S. Shavell, *The Uneasy Case for Product Liability*, 123 Harvard Law Review 1438 (2010).
[3] *Consumer Protection and the Criminal Law*, 35 Journal of Criminal Law 281, 282 (1971).

'personalization' the new privacy breach now? Are consumers safe online or are even more exposed to exploitation? The release of the Consumer Protection (E-Commerce) Rules, 2020, can be seen as a step taken by the Government to ensure the protection of the consumer on online platforms. The said Rules should be put through the legal lens to prefigure the success of its objective. Furthermore, misleading advertisements are a leading factor that impact consumer loyalty, safety as well as confidence. With false claims of curing diseases or the false guarantee of warranty of electronic products, innocent consumers often get duped. It is also pertinent to note that consumer confidence was at an all-time low in March 2020, right before the lockdown[4] and the survey initiated in January 2021 by the RBI would reveal the reverberations of the pandemic on the Indian consumer.[5] This journal is a humble attempt to answer the questions raised on consumer rights and protection in India. The horizon has to be broadened to discern what the future holds for the average Indian consumer and what are the possible legal safeguards and remedies that should be taken into consideration.

In the context above, Saikrishna & Associates is pleased to present Volume 7 Issue 1 of RGNUL Student Research Review Journal ("**RSRR**"). We would like to express our sincere gratitude to all professionals, academicians and students who have taken out the time to present their valuable perspectives and opinions, adding to the discussion of the hour. As an organization extending its arm into academic endeavors, we are glad to have received submissions ranging from complex issues of privacy, Artificial Intelligence and dark patterns to intricacies of new law vis-a-vis product liability, education and much more.

We are delighted to have shared the enormous experience and contributed to the success of this journal, alongside the dedicated set of students in the Editorial Board. We commend their perseverance and hard work to curate the journal when consumer issues are rising more than ever, despite the hurdles created by the pandemic. We congratulate the Editorial Board of RSRR for this outstanding initiative and wish them success in all their future endeavors.

We hope that our inquisitive readers have an enriching escapade and become a part of the discussion!

Saikrishna & Associates

---

[4] *Consumer Confidence Survey,* Reserve Bank of India, available at https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=19434, last seen on 04/03/2021.

[5] *RBI launches the January 2021 round of Consumer Confidence Survey,* Reserve Bank of India, available at https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=50905, last seen on 04/03/2021.

TABLE OF CONTENTS

LONG ARTICLES

UNPACKING DARK PATTERNS: UNDERSTANDING DARK PATTERNS AND THEIR IMPLICATIONS FOR CONSUMER PROTECTION IN THE DIGITAL ECONOMY

[*]Beni Chugh & [**]Pranjal Jain

ABSTRACT

This paper examines the increasing use of dark patterns in digital interfaces and the concerns they raise for consumer protection. Dark patterns are user-interfaces that confuse, coerce, or manipulate users into making a decision that does not reflect their underlying preferences. By exploiting users' cognitive biases and reinforcing users' information asymmetry, dark patterns impair their decision-making abilities. They coerce users into disregarding their preferences and acting against their best interests. This can cause significant harm in rapidly digitizing economies and societies. Dark patterns are already being used to steer users to sign up for financial products they may not need. They are also influencing citizens' political choices and interfering with democratic processes. These incursions into users' autonomy significantly disenfranchise and disempower them in the digital economy. Further, emerging research suggests that users with lower levels of education and earning lower levels of income are more vulnerable to dark patterns. These findings are crucial for jurisdictions such as India where the use of the internet is fast expanding to rural parts, and there is a rise in first-generation users of the internet.

Here we analyze the use of dark patterns in digital interfaces and the influence they exert on users' decision making. It distinguishes dark patterns from persuasive advertisements and sets out a list of common dark patterns to examine their adverse consequences for consumers. It advocates for regulatory intervention to arrest the proliferation of dark patterns on the internet and remedy the power imbalance they have already wrought. It concludes with some open questions that India must contend with when regulating dark patterns.

[*] Beni Chugh, Research Manager, Future of Finance Initiative at Dvara Research.
[**] Pranjal Jain, Co-founder of theUXWhale, Alumnus of Dvara Research.

I. INTRODUCTION TO DARK PATTERNS

Until recently it was common for travel portals to bundle travel insurance with travel tickets. They used pre-checked boxes to default the user into buying the insurance cover, even when the user had shown no active interest in purchasing the product or understanding it. Exhibit 1 demonstrates a screenshot of a transaction, typical of travel portals in India until recently.

Exhibit 1: Use of pre-checked buttons to bundle insurance cover with travel tickets | Source: *MoneyControl*[1]

This use of pre-checked buttons to bundle travel cover with travel tickets is a classic example of a 'dark pattern'. Dark patterns are *"user interfaces that make it difficult for users to express their actual preferences or that manipulate users into taking actions that do not comport with their preferences or expectations"*.[2] The term 'dark pattern' was coined by Harry Brignull in 2010, who defined it as interface designs that *"trick users into doing things that they might not want to do, but which benefit the business in question*".[3] Dark patterns use the design of the interface to influence users to make choices they would not have made if

[1] *Explained: Here is why airlines, portals can no longer mis-sell you travel insurance from Oct 1*, Moneycontrol, available at https://www.moneycontrol.com/news/business/economy/explained-here-is-why-airlines-portals-can-no-longer-mis-sell-you-travel-insurance-from-oct-1-4492451.html, last seen on 23/12/2020.

[2] *Stigler Committee on Digital Platforms, Final Report,* Stigler Committee, available at https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf?la=en, last seen on 23/12/2020

[3] H, Brignull, *Dark Patterns: inside the interfaces designed to trick you*, The Verge, available at https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you, last seen on 23/12/2020.

the user interface did not distort the information presented to the user or limit the user from acting on that information.

In the example above, the use of pre-checked boxes assumes that the user's default preference will be to purchase an add-on financial service. Users are expected to expend costly time and attention to uncheck the box and opt out of the default purchase. This default setting is unfair and taps into users' cognitive limitations. Users are known to be less likely to opt-out of existing defaults as they are beset by several cognitive biases and severe cognitive inertia, that keep them from questioning default options.[4] Research from other jurisdictions suggests that when travel insurance covers travel tickets, even those users who did not intend to buy the cover, end up buying it. Even more worryingly, a sizeable proportion of buyers remains unaware that they purchased the cover, implying that they may never actually benefit from the insurance.[5]

Recognizing that pre-checked boxes disempower users by leveraging their cognitive biases, the Insurance and Regulatory Development Authority of India ("**IRDAI**") has prohibited travel portals in India from using them for selling travel insurance. IRDAI has directed travel insurance companies to "*ensure that any portal or App providing the travel insurance coverage shall not pre-select the option of buying the travel cover as a default option*".[6] The regulator further emphasized that prospective buyers of insurance products should be allowed to make an "*informed choice"* before buying them. This regulatory

[4] *General Insurance Add-Ons Market Study – Remedies: banning opt-out selling across financial services and supporting informed decision-making for add-on buyers*, Financial Conduct Authority, UK, available at https://www.fca.org.uk/publication/policy/policy-statement-15-22-general-insurance-add-ons.pdf, last seen on 23/12/2020; E.J. Johnson, S. Bellman & G.L. Lohse, *Defaults, Framing and Privacy: Why Opting In-Opting Out*, 13 Marketing Letters 5, (2002), available at https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf, last seen on 23/12/2020; *Consumer Rights Directive*, Brussels: European Commission, available at https://ec.europa.eu/info/policies/consumers/consumer-protection_en, last seen 23/12/2020.

[5] *General insurance add-ons: Provisional findings of the market study and proposed remedies*, Financial Conduct Authority, available at https://www.fca.org.uk/publication/market-studies/ms14-01.pdf.

[6] *Circular on Travel Insurance Products and operational matters*, IRDAI, available at https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo3913&fl, last seen on 23/12/2020.

intervention shines a light on the increasing use of dark patterns and the questions it raises for consumer protection in the digital economy.

II. EFFECT OF DARK PATTERNS ON USERS' DECISION-MAKING ABILITIES

Dark patterns differ from other marketing strategies in the effect they have on users' preferences. Their objective is to make consumers disregard their own preferences and act in a manner inconsistent with them. They are designed to be manipulative rather than persuasive,[7] to encourage users to make decisions they would not have made if not for their influence. This is in sharp contrast to persuasive marketing efforts that influence users to revise their preferences.[8] This is evident in the example of the bundling of travel insurance cover with the travel ticket. The travel portal does not introduce the buyers to the product or convince them of its utility to influence their preferences. Instead, it resorts to directly adding the travel cover to the buyer's purchase, regardless of their preferences.

A growing body of scholarship is investigating the effects of dark patterns on the decision-making process of users by drawing on Tversky & Kahneman's Dual Process Theory.[9]Kahneman & Tversky's research suggests that humans have two modes of thinking: *System* 1 thinking and *System 2* thinking. *System 1* thinking is prompt, unconscious, automatic, less laborious, and less rational. *System 2* thinking tends to be more conscious, rational and laborious. Researchers suggest that dark patterns appeal to *System 1* of the human brain, encouraging users to make impulsive decisions that could serve the interests of the providers better than the interests of the users.[10]

---

[7] Supra 2.

[8] J. Luguri & L. Strahilevitz, *Shining a light on Dark Patterns*, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879 (2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205, last seen 23/12/2020.

[9] A. Tversky & D. Kahneman, *Judgment under Uncertainty: Heuristics and Biases,* 185 Science 1124, 1131 (1974).

[10] C. Bösch et al., *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 2016 Proceedings on Privacy Enhancing Technologies, 237–254 (2016); J. Luguri & L. Strahilevitz, *Shining a light on Dark Patterns*, University of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879 (2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3431205, last seen 23/12/2020.

Users' decisions are influenced by the way information is presented to them. Features of the design interface such as the language in which information is presented, the functional hierarchy including the placement of the information, the font type, size and color used to present the information, influence the users' decisions. Digital interfaces and accompanying choice architecture can be used to exploit users' cognitive vulnerabilities. The choice architecture is informed by a deep understanding of the users' behavioral biases, their bounded rationality, cognitive inertia and the constraints on the time and attention of users when they make decisions. As expert depositors in the Federal Trade Commission ("**FTC**") submitted, dark patterns are designed through extensive research and A-B testing. Designers experiment with interface designs and choose the ones most likely to distort the information and choices available to the users and cloud their decision-making. As a result, consumers' "*choice opportunities are just completely muddled and clouded by the little tricks that companies play*".[11]

Pre-checked boxes are one such design feature. Other design features include the careful wording of users' options and the choice of font color and the placement of buttons to close windows or to skip ads. For instance, IRDAI's ban on pre-checked boxes does not prevent the travel portal from deploying other forms of dark patterns to manipulate the consumer into buying the product. Portals pay special attention to the language used to frame users' choices. Exhibit-2 demonstrates this wordplay, where the option to refuse the purchase of the travel insurance is crafted as "*I am willing to risk my trip*". This creates a sense of fear among consumers and guilts them into revising their choices– a dark pattern identified as '*confirmshaming*'.[12]

[11] *Competition and Consumer Protection in the Twenty-First Century*, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_1_4-9-19.pdf, last seen 24/12/2020.

[12] *What are dark patterns?,* Dark Patterns, available at https://www.darkpatterns.org, last seen on 24/12/2020.

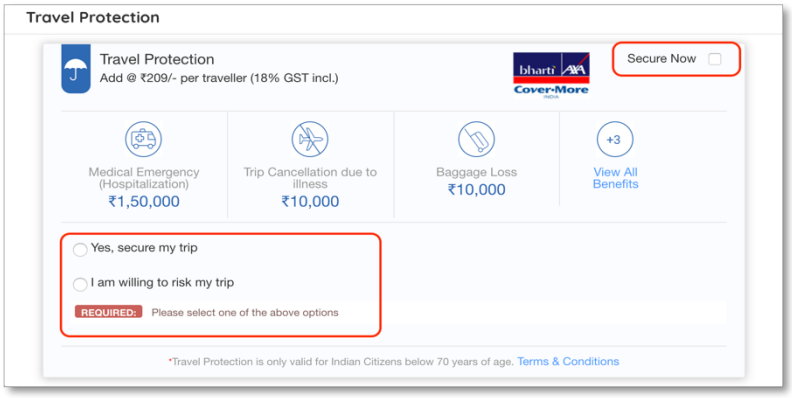

Exhibit 2: The option of not buying the insurance product is worded as "I am willing to risk my trip". This articulation creates a fear and guilt in the consumer, coercing them into compliance. This is 'confirmshaming'.

Source: Screengrab from a leading travel portal in India.

Though coercive practices in advertisements are not new, dark patterns raise concerns because of the scale and pervasiveness of their use. The prevalence of dark patterns across the web is unknown quantitatively, but a recent study[13] examined dark patterns on a set of most popular e-commerce websites. The study included 53,000 product pages across 11,000 shopping websites, and it found over 1,800 instances of dark patterns being deployed by these websites. The study suggests that these digital retailers used dark patterns to trick users into buying products they did not want. The following section discusses some typical dark patterns and the adverse outcomes they create for consumers.

III. SOME TYPICAL DARK PATTERNS AND THEIR IMPLICATIONS FOR CONSUMER OUTCOMES

Dark patterns steer users to give precedence to the providers' interests over their own. Our analysis suggests that digital service providers benefit from: (i) maximizing the sale of their product or service and/or, (ii) maximizing the personal information they collect from the user. The first objective of maximizing sales is not unique to digital service providers. The second objective of maximizing personal information has heightened relevance for

[13] A. Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 Proceedings of the ACM on Human-Computer Interaction (2019).

digital service providers. In the digital economy, it is a common practice for providers to offer products and services at zero monetary prices. Even when consumers do not pay a monetary price for the services they consume, it is well established that consumers compensate digital providers with their personal data.[14] The value of users' personal information for digital service providers can be best gauged by the fact that most Big Tech companies generate a sizeable portion of their revenues from the sale of advertising.[15] Further, the prices they command from advertisers are positively correlated with the variety and depth of personal information they have on prospective buyers.[16] Some dark patterns seek to influence the user into buying products and subscribing to services, or giving away more personal information than they would prefer. We classify these adverse effects of dark patterns into:

i. perpetuating deceptive and unsuitable selling practices, and
ii. nudging consumers to share excessive personal information.

1. Perpetuating Deceptive and Unsuitable Selling Practices

Dark patterns proliferate deceptive and unsuitable selling practices by:

1.1 Subscribing the user to a product or service she did not want

These techniques deceive the user into buying products or services that they did not intend to buy. Some typical dark patterns used to achieve deceptive sales include *sneak in the basket, forced continuity, urgency* and *scarcity*. *Sneak in the basket practices* use pre-checked boxes to trick consumers into buying products or services without some affirmative action or informed consent on part of the user. *Forced continuity* practices deceive the users into subscribing to paid subscriptions at the end of free trials. It uses credit card details taken at the time of free trial to automatically subscribe users to paid services without warning or requiring any affirmative action from them.

[14] *Quality Considerations in Zero Price Markets*, The OECD, available at https://one.oecd.org/document/DAF/COMP(2018)14/en/pdf, last seen 24/12/2020.
[15] Ibid.
[16] D. Srinivasan, *The Antitrust Case Against Facebook*, 16 Berkeley Business Law Review Journal (2019).

Similarly, *urgency* and *scarcity* practices are used to create the impression of scarcity to make the user purchase a product or service.

1.2 Subscribing user to a product or service that is not in their best interest

These selling practices nudge the user to act against their best interests by choosing products or services that may not be beneficial to them. This is typically encouraged by using dark patterns that hide information crucial for decision-making such as the true costs of the product (a dark pattern called *hidden costs),* add irrelevant choices to distract users (*misdirection*), guilt the users into making a choice not beneficial for them (*confirmshaming*) or by asymmetric presentation of choices.

Asymmetric presentation of choices in the case of dynamic currency converter has been a burning consumer protection issue in the European Union ("**EU**"). Travelers on international trips are often confronted with a choice to make payments using their native currency or the local currency of the destination. Buyers are naturally disposed to pay in their native currency because of their comfort with it. However, payments in native currency abroad often make the transaction expensive for the buyers because they attract conversion costs. Simultaneously, providers stand to gain by the additional conversion fee. Consumer groups across the EU have underscored providers' tendency to subtly encourage the users to pay in the more expensive native currency by presenting this option in a benign 'green color' as illustrated in Exhibit 3. This reinforces consumers' cognitive bias associated with the color green and encourages users to make payments in the more expensive native currency.[17]

[17] *Dynamic Currency Conversion: When paying abroad costs you more than it should*, The European Consumer Organization, available at https://www.beuc.eu/publications/beuc-x-2017-118_dynamic_currency_conversion_position_paper.pdf, last seen 24/12/2020.

Exhibit 3: ATMs in EU Countries.

1.3 Making it harder for the consumer to discontinue or opt-out of existing purchases and subscriptions

Dark patterns are also used to retain consumers in ongoing services by making it harder for them to discontinue or opt-out of existing subscriptions. The 'Roach Motel' dark pattern is used to keep users subscribed to services by requiring them to go through several pages before they can opt-out. It resembles the classic maze in which entering a maze is easy but finding the right path out is much more difficult.[18] 'Roach Motel' is used while designing interfaces for cancelling subscriptions, deactivating accounts or unsubscribing from a mailing list.

2. Nudging Consumers to Share Excessive Personal Information

In a rapidly digitizing economy, users' data is an important economic input[19] and providers seek to maximize the data collected from users. Dark patterns such as 'Privacy Zuckering' (encouraging users to share more personal information publicly) and 'Trick Questions' (tricking users into giving answers they did not intend to) sway users into sharing more personal data than they intended to. A recently concluded study shows that

[18] Supra 12.
[19] *The economic value of data: discussion paper*, Government of United Kingdom, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf, last seen on 24/12/2020.

dark patterns can set back the effectiveness of consent management platforms. Removing the opt-out button from the first page of the notice increases instances of users giving consent by over 22 percent.[20]

In concluding this discussion on typology, the table below summarizes the most prevalent dark patterns found in our review of literature and their effects on consumers' outcomes.

Dark Pattern	Description	Intended effect on users
Sneak in the basket	Tricks users into buying products without their informed consent.	Subscribes users to unwanted products or services.
Forced continuity	Deceives users into subscribing to paid subscriptions via free trials.	Subscribes users to unwanted products or services.
Expensive autorenewals	They renew subscriptions to the most expensive business models.	Subscribes users to services that are not in their best interest.
Urgency	Makes users believe that purchases are urgent.	Manipulates users to subscribe to products or services.
Scarcity	Makes users believe that products are scarce.	Manipulates users to subscribe to products or services.

[20] *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence,* Honolulu: Association for Computing Machinery, available at https://arxiv.org/pdf/2001.02479.pdf.

Hidden costs	Hides true costs of products.	Subscribes users to services that are not in their best interest.
Misdirection	Adds irrelevant choices to confuse users.	Subscribes users to services that are not in their best interest.
Confirm shaming	Guilts users into buying products.	Subscribes users to services that are not in their best interest.
Asymmetric presentation of competing choices	Represents competing choices asymmetrically, making one look more appealing than the other.	Manipulating the user to make a choice that may not be in their best interest.
Roach motel design	Makes it hard to unsubscribe a product or service or abort transactions.	Subscribes users to unwanted products or services.
Privacy Zuckering	Encourages users to share more personal information publicly.	Encourages users to share excessive personal information.
Trick Questions	Tricks users into giving answers they did not intend to.	Encourages users to share excessive personal information.

Table 1: Some common dark patterns and their effect on consumers' outcomes.

Source: Compiled by the authors based on their review of the literature.

IV. DARK PATTERNS: A CALL FOR ACTION TO REGULATORS?

The decision to regulate dark patterns rests on at least two important considerations- (i) the inability of users to safeguard themselves from dark patterns, and (ii) the inability of market competition to penalize the use of dark patterns.

1. The Inability of Users to Safeguard Themselves from Dark Patterns

Although empirical research on the effect of dark patterns on consumers is still quite young, a recently concluded American study examines the efficacy of a bait and switch dark pattern that persuaded users to buy an identity theft protection plan.[21] The experiment, conducted on a group of over 1900 respondents, found that the respondents' willingness to enroll into identity theft protection plan was significantly and positively related to their exposure to dark patterns. The respondents' enrolment rates in the identity theft protection program more than doubled when they were exposed to mild dark patterns, while it quadrupled for those exposed to aggressive dark patterns.

More worryingly, the findings of this study also show that respondents with lower levels of education are more vulnerable to dark patterns. In the control group (i.e., in the absence of dark patterns) level of education of respondents did not affect their decision to enroll in the program. However, in the presence of dark patterns, respondents with lower levels of education exhibited higher rates of enrolment. The study also found that respondents with low levels of income are likely to be more influenced by dark patterns. These findings emphasize that individuals belonging to disadvantaged and marginalized groups are more vulnerable to dark patterns.

This has significant implications for India, which is characterized by low income, low levels of digital literacy and a sizeable proportion of first-time users of the internet. Journalistic reports suggest that individuals with lower levels of education and in urgent need of money make for easy targets for financial service providers. Often users also sign-up for financial products unintentionally and unknowingly. Notably, an ed-tech company, Byju, offered loans to hundreds of unsuspecting parents at the time of enrolling their children for online coaching classes. The parents' biometric impressions taken at the time of enrolment were used to give them loans that they had not sought. Of the small sample of the parents examined in

[21] Supra 8.

this report in 'The Ken', 50 percent had no information that they had purchased a loan in the guise of a free trial.[22]

Similarly, it is also common for users to face significant deterioration in their financial condition because they signed-up for financial services without fully knowing their terms and conditions.[23] Though these are instances of mis-selling of products in traditional finance, these are likely to get worse when first-generation digital users are influenced by dark patterns while accessing digital finance.

2. The Inability of Market Competition to Penalize the use of Dark Patterns

Competition in markets is a powerful tool to uphold consumer protection.[24] Competition in markets enables consumers to choose from a wide variety of providers and reject providers that offer inferior products. This incentivizes providers to compete on the quality of the product. However, market failures that arise when providers' incentives are not aligned with the consumers' best interest are unlikely to be redeemed by competition. This appears to be true of dark patterns. Although the empirical research is still quite new and limited, it is beginning to show the limitations of market competition to address dark patterns.

In their ground-breaking study, researchers from Princeton found that shopping websites that were more popular as per Amazon's Alexa rankings were more likely to deploy dark patterns.[25] Similarly, the American study discussed earlier found that the use of mild dark patterns by digital providers is likely to go unpunished.[26]

---

[22] *The making of a loan crisis at Byju's*, The Ken, available at https://the-ken.com/story/the-loan-crisis-at-byjus/, last seen on 24/12/2020.
[23] *Selling to those who can't pay: human cost of modern banking*, The Ken, available at https://the-ken.com/story/human-cost-of-modern-banking/?utm_source=daily_story&utm_medium=email&utm_campaign=daily_newsletter, last seen 24/12/2020.
[24] *Indian Financial Code*, Financial Sector Legislative Reforms Commission, available at https://dea.gov.in/sites/default/files/fslrc_report_vol2_1.pdf, last seen 25/12/2020; *Report of the Financial Sector Legislative Reforms Commission*, Government of India, available at https://www.prsindia.org/report-summaries/financial-sector-legislative-reforms-commission, last seen 25/12/2020.
[25] Supra 13.
[26] Supra 2; Supra 8.

In summary, emerging evidence suggests that dark patterns are fast becoming an instrument of competition rather than competition being a restraint on the use of dark patterns. The market mechanism *per se* may be inadequate to address the consumer protection concerns raised by dark patterns. Simple, subtle dark patterns that are effective in manipulating the consumer attract little or no backlash from the consumers. Consequently, they appear to be increasingly prevalent among popular service providers. Moreover, though dark patterns diminish users' autonomy and welfare across the board, their effects are more pronounced for the already disadvantaged groups such as those with lower levels of education.[27]

V. CONCLUSION: OPEN QUESTIONS FOR REGULATORS WHEN REGULATING DARK PATTERNS

Discussions so far indicates that the use of dark patterns warrants regulatory intervention. However, regulatory approaches to dark patterns must contend with a few frontier questions:

1. Distinguishing between Personalization and Manipulation

The distinction between personalization and manipulation has been at the heart of policy issues that stem from the use of personal information in the supply of services. Moreover, the distinction between personalization and manipulation is subject to the social-cultural context of the users, their own privacy preferences and the outcome of the interface design. As an example, using behavioral data to understand users' preferred payment methods and modifying the interface to present the most-used payment method upfront may reduce friction in users' payment experience and increase convenience. However, if that preferred-payment mode attracts an additional transaction fee then many would argue that the interface's design amounts to dark patterns. The line between personalization and manipulation is not only thin but it is also murky because it is fraught with subjective assessments of the designer's intentions, implications for consumer welfare and the consumer's own value system.

[27] Supra 2.

An exclusively objective standard of distinguishing personalization from manipulation may not be feasible or even warranted. Scholarship from behavioral economics can lend some ideas on creating a framework to distinguish manipulative dark patterns from benign nudges. Thaler and Sunstein define nudges as "*any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives*".[28] Their emphasis on the effect of a nudge being predictable and not changing users' economic incentives could serve as important indicators for identifying dark patterns which are likely to fail on one or both counts.

It is crucial that a framework to identify dark patterns incorporates and reflects society's expectations, value-system, and cultural context. The community's engagement is essential to determine choices that cannot be squarely addressed by the law and where the trade-offs are more intricate. For instance, in our small but deeply qualitative study in 2017, respondents unequivocally expressed their reservations against providers using their location data.[29] These findings were also corroborated by other primary studies, such as those undertaken by Consumer Unity and Trust Society[30] ("**CUTS**"). Any default settings that permit providers to collect users' location data when it is not strictly necessary to provide a service will be adjudged as a dark pattern. Any determination of dark patterns cannot be made in isolation from the socio-cultural context and with disregard for the community's perceptions. To achieve this, regulators must crowd-in opinions from the community, engage in inclusive public consultations, conduct primary studies to gauge users' privacy preferences and be transparent about their decision-making processes.

2. Appointing Appropriate Regulatory Body to Regulate Dark Patterns

[28] R. Thaler & C. Sunstein, *Nudge - Improving Decisions About Health, Wealth, and Happiness*, 6 (2008).
[29] *Privacy on the Line*, Dvara Trust, available at https://www.dvara.com/research/wp-content/uploads/2017/11/Privacy-On-The-Line.pdf, last seen 25/12/2020.
[30] *Is privacy an elitist concern? Not so, says new survey*, The Scroll, available at https://scroll.in/article/899168/is-privacy-an-elitist-concern-not-so-says-new-survey, last seen 25/12/2020.

Appointing a relevant regulator to oversee dark patterns is not straightforward. Dark patterns could attract several regulators' jurisdictions simultaneously. Regulators with direct jurisdiction over dark patterns include a data protection authority, the consumer protection authority and the sectoral regulator(s) that has jurisdiction over the provider using dark patterns. Simultaneous jurisdiction can lead to duplication of regulation or regulatory arbitrage.

The IRDAI did not have jurisdiction over travel portals, in the example of travel portals using prechecked boxes to sell insurance cover. It had to rely on regulated entities i.e. travel insurance providers to enforce the ban, as also reflected in its language, "*Insurers shall ensure that any portal or App providing the travel insurance coverage shall not pre-select the option of buying the travel cover as a default option"*.[31] While the regulator was able to achieve its objectives in this case, it does highlight the problem that sectoral regulators may not have jurisdiction over e-commerce entities or social networking platforms. This can create a patchy regulatory framework and may not protect users effectively from the use of dark patterns.

The existing consumer protection authority is emerging as a strong contender to regulate dark patterns due to its economy-wide jurisdiction. In the United States, the Federal Trade Commission ("**FTC**") which is the federal body in charge of consumer protection in the economy has been regulating dark patterns and penalizing service providers by using its power to punish "*unfair and deceptive practices"*.[32] The case of *Federal Trade Commission* v. *AMG Capital Management*[33] is an important ruling on dark patterns. AMG Capital Management, a payday lender, deployed dark patterns to auto-renew (instead of close) expensive payday loans to borrowers. Borrowers were deceived into believing that their loans would be closed after withdrawing the principal amount and the interest rate in one instalment from their bank account. The interface, however, was not designed to close the loan. Prechecked boxes in the loan agreement ensured that the default

[31] Supra 6, S. 3(iii).
[32] 15 U.S.C. S. 5 (United States).
[33] Federal Trade Commission v. AMG Capital Management, 19-503 (2021, United States Court of Appeals for the 9th Circuit).

option was set to auto-renewal of the loan. Auto-renewals directed users to more expensive subscription models, and, Roach Motel models ensured that users could not change the extortionist default settings easily.[34] The FTC found AMG Capital Management guilty of unfair and deceptive practices under Section 5 of the FTC Act. The Court of the Appeals of the Ninth Circuit also upheld the FTC ruling, and the amount of penalty (USD 1.3 bn) levied on the provider.[35]

The language of the FTC Act and its interpretation of deceptive practices allowed the FTC to book the offender and punish them for their misconduct. The success of existing consumer protection authorities in regulating dark patterns will depend on the language of the existing regulation and its ability to include dark patterns in the cause of action. In India, some dark patterns such as *hidden costs* could fall under the remit of the Consumer Protection Act, 2019 and the Central Consumer Protection Authority ("**CCPA**") that the Act creates to redress such issues. Section 11(ii) of that Act considers the deliberate withholding of important information as a deficiency in service that is punishable under the Act. Similarly, Section 28(iv) of the Act considers it as 'misleading advertisement'. Other dark patterns such as *confirmshaming*, however, are harder to fit into this consumer protection framework. The inability to qualify these dark patterns as offences under the consumer protection framework could significantly constrain the regulator's effectiveness in regulating their use.

To overcome these issues, existing consumer protection frameworks could be amended to equip them to deal with dark patterns. American senators introduced the 'Deceptive Experiences to Online Users Reduction ("**DETOUR**") Act'. This Bill aims to curb the use of dark patterns by banning interface features that intentionally diminish consumers' autonomy, ability to make decisions and choices. It also gives the FTC more authority to regulate such practices and provide guidelines to

[34] Supra 8.
[35] Supra 33.

platforms on design practices.[36] Consumer protection bodies with amended legislations that allow them to regulate for dark patterns could help in creating a consistent consumer protection framework. It could also spare consumers the anxiety of navigating a new regulatory body with a new set of mechanisms.

3. Designing Effective Regulatory Tools to Regulate Dark Patterns

Designing appropriate regulatory tools is crucial to the success of regulators. Considering that regulating dark patterns is a recent regulatory preoccupation, there is limited research on the tools that regulators could use to address it. Some tools that appear useful from the preliminary analyses of issues and emerging research include:

3.1 Auditing of organization's design practices

Regulators can periodically audit digital interfaces to gauge the effect of the interfaces on users' decision-making capacity and agency. Audits could look for designs that foster deceptive and unsuitable selling or nudge users to share excessive personal information. Lessons can be drawn from the audits designed to prevent algorithmic bias as a way to promote compliance in the automated systems.[37] As algorithms become more embedded in decision-making in the economy, providers are leaning on researchers and journalists to examine their algorithms for discrimination.[38] Similar collaborations could be explored to audit digital interfaces for dark patterns. In addition to audits, regulators could also lay out model

---

[36] *Senators Introduce Bipartisan Legislation to Ban Manipulative 'Dark Patterns'*, Mark R. Warner, US Senator from the Commonwealth of Virginia Website, available at https://www.warner.senate.gov/public/index.cfm/2019/4/senators-introduce-bipartisan-legislation-to-ban-manipulative-dark-patterns, last seen on 26/12/2020.

[37] B. Casey, A. Farhangi & R. Vogl, *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, 34 Berkeley Technology Law Journal 143 (2018), available at https://ddl.stanford.edu/sites/g/files/sbiybj9456/f/Rethinking%20Explainable%20Machines.pdf, last seen on 25/12/2020.

[38] *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms*, University of Michigan, available at http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf, last seen on 25/12/2020.

interfaces or guidelines to help providers design user-friendly interfaces, such as those set out by the IRDAI or the FTC. Regulators could also mandate a design practice where the opt-in and opt-out choices presented to the users are equal in hierarchy and comprehensible for all users. These guidelines may be especially relevant when regulators rely on digital interfaces for enforcing laws. For instance, the effectiveness of the German law to regulate hate speech online- the 'Netzwerkdurchsetzungsgesetz' ("**NetzDG**" or the "**Network Enforcement Act**"), was significantly compromised because of dark patterns. The law mandated social networks to offer users a form to report unlawful content online. In some cases, significant providers with millions of users made the pathway to reporting hate speech lengthy, convoluted, and requiring multiple clicks from users. This reduced reporting incidents and considerably reduced the effectiveness of the Act.[39]

3.2 Developing bright-line rules to detect dark patterns

Creating bright-line rules, i.e., objective standards to detect dark patterns can help regulators remove ambiguity around what is permissible. These standards can be a crucial benchmark against which user interfaces can be measured to assess if they exert undue influence over users' autonomy. Further, bright-line rules should reflect the users' ideal expectations of the providers. A-B testing of interfaces should not only be conducted to maximize providers' interests[40] providers could also solicit users' feedback on the design interface to make it user friendly.

Dark patterns can enable the economic exploitation of users and their disenfranchisement by limiting users' ability to exercise their rights on digital interfaces and vitiates regulation. Together, these possibilities highlight the need and urgency to regulate dark patterns. The urgency is warranted by the disproportionate effect that dark patterns are likely to wield on users from disadvantaged and marginalized groups. This is especially relevant for demographics such as rural internet users in India,

[39] S. Reigers & C. Sanders, *Dark Patterns: Regulating Digital Design* (Berlin: Stiftung Neue Verantwortung 2020); *Dark Patterns and Policy*, Data and Society Points, available at https://points.datasociety.net/dark-patterns-and-design-policy-75d1a71fbda, last seen on 25/12/2020.

[40] Supra 11.

who have started to outnumber urban users.[41] With significantly less exposure to the internet, lower levels of literacy and potentially lower levels of awareness about dark patterns, these users are more vulnerable to their deployment by providers.

The government's push for digitization in the last decade will lack legitimacy if digital interfaces cannot be safe for users. Rural respondents in our primary study, Privacy on the Line*,* emphasized their inability to comprehend or audit providers' practices on digital interfaces and the lack of agency and means to demand recourse from them. The respondents in our study unanimously emphasized the need for a guarantee that the providers' activities will not harm them and the need for the government to intervene should harm occur.[42] Given the expansion of the internet to first-time users, the policy push for digitization and the users' demand for more safeguards in the digital economy, the call for action to regulators cannot be stronger.

References:

Justice Srikrishna committee submits report on data protection. Here're its top 10 suggestions, Econmic Times, available at https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms.

India's Personal Data Protection Bill: What we know so far, MoneyControl, available at https://www.moneycontrol.com/news/technology/indias-personal-data-protection-bill-what-we-know-so-far-4297331.html.

Dark patterns in UX: how designers should be responsible for their actions, UX Collective, available at https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c.

Johnson, E. J., Bellman, S., & Lohse, G. L, *Defaults, Framing and Privacy: Why Opting In-Opting Out,* 15 Columbia University Faculty Research, 5, 15

[41] *India has more internet users in rural areas than urban: IAMAI report*, The Hindustan Times, available at https://tech.hindustantimes.com/tech/news/india-has-more-internet-users-in-rural-areas-than-urban-iamai-report-story-1EsbphWTBM5wZzjtNFXXyJ.html, last seen on 25/12/2020.

[42] Supra 28.

(2001), available at https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf.

The economic value of data, Government of UK, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731349/20180730_HMT_Discussion_Paper_-_The_Economic_Value_of_Data.pdf.

Personal Data: The Emergence of a New Asset Class, World Economic Forum, available at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

How Businesses Are Collecting Data (And What They're Doing With It), Business News Daily, available at https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

Cooper, J, *Personalization: The Key to Monetizing Your Content*, Adobe Blog, available at https://theblog.adobe.com/personalization-key-monetizing-content/.

Wilson, S, *Every Cognitive Bias Put Into a Single Diagram*, Clinically Relevant Insights BLOG, available at https://www.shawnwilsonphd.com/post/2017/10/06/every-cognitive-bias-put-into-a-single-diagram.

Should Restaurants Offer Healthy Menu Options?, The Balance Small Business, available at https://www.thebalancesmb.com/should-restaurants-offer-healthy-menu-options-4147177.

Lai, Y.-L., & Hui, K.-L, *Internet opt-in and opt-out: investigating the roles of frames, defaults and privacy concerns*, SIGMIS CPR '06: Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research, 253, 263 (2006).

Hanson, J. D., & Kysar, D. A. (1999), *Taking Behavioralism Seriously: Some Evidence of Market Manipulation*, 112 Harvard Law Review 149 (1999).

Luo, S., Gu, B., Wang, X., & Zhou, Z., *Online Compulsive Buying Behavior: The Mediating Role of Self-control and Negative Emotions*, ICIEB '18: Proceedings of the 2018 International Conference on Internet and e-Business. Singapore: Association for Computing Machinery (2018).

Zhang, F., Yuan, N. J., Zheng, K., Lian, D., Xie, X., & Rui, Y., *Mining consumer impulsivity from offline and online behavior,* UbiComp '15: Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing Osaka Japan: Association for Computing Machinery (2015).

Luo, X., *How Does Shopping with Others Influence Impulsive Purchasing?* 15 Journal of Consumer Psychology 288-294 (2005).

Calo, R., *Digital Market Manipulation*, 82 George Washington Law Review 57 (2019).

Google Location Services: Spam, UXP2 - Dark Patterns, available at https://darkpatterns.uxp2.com/pattern/google-location-services-spam/.

Unfair and Deceptive Trade Practices, Mass Legal Help, available at https://www.masslegalhelp.org/consumer/unfair-deceptive-trade-practices.

User-Centered Design Basics, Usability.gov, available at https://www.usability.gov/what-and-why/user-centered-design.html.

Frederick, S., Loewenstein, G., & O'Donoghue, T., *Time Discounting and Time Preference: A Critical Review*, 40 Journal of Economic Literature 351, 401 (2001).

Confirmation bias, Science Daily, available at https://www.sciencedaily.com/terms/confirmation_bias.htm.

Prasad, S., *Defining "Harm" in the digital ecosystem,* Dvara Research, available at https://www.dvara.com/blog/2019/05/06/defining-harm-in-the-digital-ecosystem/.

Calo, R., *The Boundaries of Privacy Harm*, 86 Indiana Law Journal (2011).

Why is data important for business, Grow, available at https://www.grow.com/blog/data-important-business.

Akerlof, G. A., *The market for "lemons": Quality uncertainty and the market mechanism. In Uncertainty in economics*, 84 The Quarterly Journal of Economics, 488, 500 (1970).

How to Monetize Your Customer Data, Gartner, available at https://www.gartner.com/smarterwithgartner/how-to-monetize-your-customer-data/.

The Data Brokers: Selling your personal information, CBS News, available at https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.

Filing complaint against Grindr's sharing users' HIV-status and sexual preferences, Forbrukerrådet, available at https://www.forbrukerradet.no/side/filing-complaint-against-grindrs-sharing-users-hiv-status-and-sexual-preferences/.

Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, available at https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower. Politico, available at https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/.

The Role of Advertising and Advertising Regulation in the Free Market, Federal Trade Commission, available at https://www.ftc.gov/public-statements/1997/04/role-advertising-and-advertising-regulation-free-market.

Hanson, J. D., & Kysar, D. A., *Taking Behavioralism Seriously: Some Evidence of Market Manipulation*, 112 Harvard Law Review 1420 (1999).

Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence, Cornell University, available at https://arxiv.org/abs/2001.024795.

INTRODUCTION OF PRODUCT LIABILITY ACTIONS IN INDIA UNDER THE CONSUMER PROTECTION ACT, 2019 - A WAY FORWARD

[*]Vagish Kumar Singh

ABSTRACT

Product liability can be broadly defined as a right of a consumer (and corresponding duty on the manufacturer or seller) to be compensated for damage or loss caused as a consequence of usage of products or services. Though familiar and akin to liability created under the Consumer Protection Act, 1986 ("Act, 1986"), the term "product liability" or any permutation thereof were absent from the Act, 1986. This absence resulted in contradictory judgments which either allowed compensation for consequential damage arising out of usage of a product or refused to entertain such claims calling them incidental and distant to the product manufacturer/ seller. Now however, the Consumer Protection Act, 2019 ("Act, 2019") has introduced a new regime of product liability and dedicated Chapter VI to further enumerate liability of a product manufacturer, product service provider or product seller. Though these provisions related to product liability can be considered as derivations from more mature product liability regimes such as those in the United States of America, differences in socio-economic and judicial systems would necessitate that Consumer Commissions implement these provisions with extreme caution and while taking guidance from best practices in other jurisdictions. This paper would examine the product liability regime introduced by the Act, 2019 specifically suggesting prudent manners of its implementation for not only ensuring just compensation and restitution to aggrieved consumers but to also regulate manufacturers, product service providers and product sellers without resorting to excess regulation by legislative intervention into every element of commerce and trade.

I. INTRODUCTION

The Consumer Protection Act, 1986 ("**Act, 1986**") was undoubtedly a proactive move towards a more transparent marketspace and sought to ensure that the Indian consumer enjoyed rights which were alien to most

[*] Vagish K. Singh, Advocate & Managing Partner, Capstone Legal.

developing countries at the time. It also roughly coincided with the opening up of the Indian economy which gradually resulted in a flood of new products & services in the marketspace which constantly led to a variety of interactions between consumers and manufacturers, sellers, retailers, service providers etc. However, it has been long understood that an entitlement to recover a purchase price or compensation if goods or services are deficient would not necessarily imply a right to claim compensation for injury which results from their usage. Such a right or rather corresponding duty on the manufacturer or seller, to compensate for damage or loss caused as a consequence of usage of products or services has been referred to as 'product liability' in common law. The Act, 1986 however never used the expression 'product liability' nor provided for any separate provision expressly dealing with such expression. The manner of enforcement of the Act, 1986 by various consumer fora however, did not reflect such inadequacy. Though the term 'consequential damage' has been sparsely used by such erstwhile fora, there are numerous instances where these tribunals have exercised their ingenuity to grant compensation for injury arising out of usage of products or services.[1] On the other hand, consumer fora have also hesitated to grant consequential damages calling such claims beyond the purview of the Act, 1986.[2] In this context, the Act, 2019 has now not only introduced definitions of product liability and expressly included a product liability action under the definition of a complaint; but the Act has also dedicated Chapter VI to product liability actions. This paper would discuss the concept and legislative structure of product liability as introduced by the Consumer Protection Act, 2019 ("**Act, 2019**") in the context of both existing jurisprudence under the Act, 1986 and experiences in more mature product liability jurisdictions, such as the United States of America ("**USA**"), and suggest a prudent manner of adjudicating over product liability actions.

[1] Asia Tea Company v. On Behalf of Commissioner, Civil Supplies and Consumer Protection Department, (2017) CPJ 461 (NC); Tata Motors v. Rajesh Tyagi, (2014) (1) CPC 267.

[2] H&R Johnson (India) Ltd. v. Lourdes Society Snehanjali Girls Hostel, (2013) CPJ 475 (NC).

II. ORIGINS OF PRODUCT LIABILITY

The foundations of product liability in English Law can be traced to jurisprudence pertaining to contractual and tortious liability. A liability under a contract for supply of goods and services primarily resorts to compensating a purchaser for unfulfilled expectations from such goods or services. Such liability though strict in nature, suffers from the requirement of privity, more specifically vertical privity.[3] Hence contractual liability would restrict remedy of a purchaser only to an immediate vendor and such was the interpretation given by English courts. A tortious liability therefore sought to ease restrictions placed by a contractual liability.[4] However, it was not until the celebrated decision of the House of Lords in *Donoghue* v. *Stevenson*[5] ***("Donoghue")*** that courts came to recognize independent and concurrent duty of manufacturers or suppliers to third parties, other than the immediate purchaser. It is argued, however, that even up until *Donoghue* courts had begun imposing a number of exceptions to non-liability due to lack of privity. Such exceptions were a natural development of case law since the market space and consumer behavior was constantly changing in more developed nations. It was becoming clearer, for example, that a supplier was to refrain from misrepresentation and disclose potential danger, prevent mishandling of hazardous goods (inherently dangerous goods) etc.[6] These principles not only formed the basis of general consumer laws as they exist today, but also contributed significantly to the development of product liability principles in the modern context. Similar to the importance that *Donoghue* holds in common law, the law of product liability in the US pivoted around the decision in *Macpherson* v. *Buick Motor Co.*[7] ***("Macpherson")***. It is also prudent to state that before *Macpherson*, courts in the USA also followed a path similar to English courts in following non-liability and general exceptions such as fraud, failure to disclose dangers etc. However, the courts in the USA expanded upon the definition of "inherently dangerous goods" more proactively. Thus, not

[3] D. Fairgrieve & R. S. Goldberg, *Product Liability*, 25 (2nd ed., 2020).
[4] Ibid at 527.
[5] Donoghue v. Stevenson, (1932) AC 562 (1932, House of Lords).
[6] Longmeid v. Holliday, (1851) 6 Ex 761 (1851, Court of Exchequer).
[7] Macpherson v. Buick Motor Co., 217 N.Y. 382 (1916, New York Court of Appeals).

only hazardous goods such as explosives or poison were considered as "dangerous in themselves", but also pharmaceuticals, food and drinks. The following passage from *Macpherson* by Justice Cardozo is worth reproducing:

> If the nature of a thing is such that it is reasonably certain to place life and limb in peril when negligently made, it is then a thing of danger. Its nature gives warning of the consequences to be expected. If to the element of danger there is added knowledge that the thing will be used by persons other than the purchaser, and used without new tests, then, irrespective of contract, the manufacturer of this thing of danger is under a duty to make it carefully.

Privity therefore came to be rightly neglected in *Macpherson* to provide protection to all reasonable users of a product. Any such user would be liable to compensation if the product was negligently made and caused peril to life and limb. In the years to follow, USA courts expanded upon the definition of 'inherently dangerous goods' and recovery was permitted even when injury was arising out of simple items such as ladders, dresses or perfume.[8] To the credit of courts in the USA, no uniform product liability statute exists in the USA and product liability claims are governed by a myriad of state, federal and common law principles. However, such lack of uniform law has not hampered development of a rich jurisprudence of product liability in the USA. Though an attempt to summarize the entirety of USA product liability laws would be a rhetorical exercise, it would be proper to state that a cause of action in product liability in the USA may be based upon negligence, breach of warranty or strict liability.[9] Negligence, as aforementioned, refers to the negligence of a manufacturer in either designing a product, manufacturing a product or in warning or instructing a consumer of uses and hazards of such product.[10]

In the Indian context, product safety and standards for specific products are governed by special legislation such as the Drugs and Cosmetics Act, 1940, Food Safety and Standards Act, 2006, Essential Commodities Act,

[8] Supra 3, at 15.
[9] M.S. Moller & P. Indig, *Products Liability Law Revisited: A Realistic Perspective*, 31(4) Tort & Insurance Law Journal 879, 882 (1996).
[10] P.A. Sexton, A.T. Suroff & L.N. McDowell, *Recent Developments in Product Liability Law*, 47(1) Tort Trial & Insurance Practice Law Journal 415, 415 (2011).

1955, Bureau of Indian Standards Act, 2016, Legal Metrology Act, 2009 among others. However, these special legislations mostly provided minimum standards and penal provisions for violation of such standards. The element of compensation to the end user who might be affected by such violation, was missing from the regulatory regime in India until the enactment of the Act, 2019.

III. PRODUCT LIABILITY UNDER THE ACT, 2019

The Act, 2019 defines product liability under Section 2(34). The essential elements of the newly introduced definition can be broken up as follows:

i. It is the duty/responsibility upon a manufacturer or product seller to compensate for harm.
ii. Harm should be caused to a consumer by a defective product or service related to such product.

The definition therefore follows a scheme which is similar to counterparts in common law by including essential ingredients of duty to compensate and consequent harm. The legislature has also made the effort to provide an inclusive definition of 'harm' under Section 2(22) specifically relating to product liability actions. Harm has therefore been defined to include damage to property, injury to person, injury to mental state/emotional state and loss of consortium. Such damage and injury should be arising out of usage of a defective product or deficient service related to such product. Reading of Sections 2(34) and 2(22) of the Act, 2019, however, appears to put an unnecessary onus on a complainant to prove that a product by which harm has been caused, was defective.

The term 'defect' and 'defective' as defined by the Act, 2019 would imply that for a product to be defective it needs to be faulty, imperfect or of inadequate quality or standard in accordance with contract or law.[11] Therefore, for harm to be compensated in a product liability claim, a consumer on a strict reading of these provisions would have to sufficiently satisfy the Commission that the product was inherently defective as per the provisions of the Act, 2019. Imposition of such a standard would be

[11] S. 2(10), The Consumer Protection Act, 2019.

contrary to established jurisprudence in the United Kingdom (**"UK"**) and the USA. It is now understood that even though a good or service may not be defective or deficient, but due to improper 'labeling', insufficient warning or instructions, harm caused from a product would fall within the domain of product liability.[12]

To address this contradiction among others, Chapter VI of the Act, 2019 has been specifically provided and dedicated to product liability actions. It is therefore imperative that while implementing provisions pertaining to product liability actions, Consumer Commissions are wary of specific provisions of Chapter VI which expand upon the strict definitions provided by the Act, 2019 as aforementioned. Accordingly, a combined reading of Sections 2(34), 2(22), 2(10) and 84 of the Act, 2019 would mean that a product manufacturer shall also be liable in a product liability action if the product fails to contain adequate instructions of correct usage or warning. Such non-inclusion of instructions or warning may not *stricto sensu* imply a defect in the product, but would invoke product liability actions and consequent liability of a manufacturer. It would be proper to state at this juncture that it would have been more appropriate to omit the word 'defective' in Section 2(34); however, in the present state of the Act, a harmonious reading of Chapter VI and Section 2(34) would be beneficial to the ultimate objective of the Act, 2019.

As aforementioned, Section 2(22) of the Act, 2019 provides an inclusive definition of 'harm' in the context of a product liability action. However, the Section also states that such harm shall not include harm to the product itself, damage to property on account of breach of warranty conditions or any commercial or economic loss. It is interesting to note that exclusion of damage due to breach of warranty conditions has been limited to damage to property. An extremely liberal reading of such exclusion would imply that injury to person, illness or death caused even on account of breach of warranty of a product would be considered as 'harm' for the purposes of a product liability action. Such liability would not only be strict i.e., irrespective of negligence on the part of the manufacturer or service

[12] M. Ursic, *Product Safety Warnings: A Legal Review,* 4 Journal of Public Policy & Marketing 80, 83 (1985).

provider, but also has the potential of negating the effect of any contributory negligence on the part of the consumer. The Consumer Commissions however, need to exercise caution while interpreting 'harm' in product liability actions. It would be prudent to suggest that a mere violation of a condition of warranty by a consumer should not exclude harm caused by a product. The alleged breach of warranty should have a nexus to the damage caused for such breach to be sufficient to discharge the manufacturer from liability. An unconnected breach of warranty conditions should not by itself convince Consumer Commissions to reject product liability claims by consumers for damage to property. On the contrary, even though breach of warranty causing injury to a person may not be expressly mentioned as an exclusion, it would be unreasonable for a manufacturer to incur liability when the sole reason or cause of personal injury was violation of a condition of warranty. It would then be imperative upon the Commission to examine whether the consequences of violation of such condition of warranty have been displayed by the manufacturer sufficiently so as to warn the consumer.

Another exclusion from the definition of harm, that warrants discussion is exclusion of commercial or economic loss. The usage of the term 'commercial' in this exclusion seems appropriate since the Act, 1986 or the present Act, 2019 are not meant to deal with disputes pertaining to commercial losses arising out of deficient goods.[13] Such commercial losses have always been the domain of contractual disputes subject to jurisdiction of commercial courts or civil courts, as the case may be.[14] However the term 'economic loss' as used in the exclusion should not be read independently of the term 'commercial', since exclusion of all economic loss from the definition of harm would lead to absurdity and defeat the purpose of introduction of the product liability provisions. A loss of income therefore should be differentiated from loss of profit; while the former may be purely an economic loss as a consequence of deficient product or services, the latter has commercial tones pertaining to expected

[13] See definition of Consumer and exclusion clause in S. 2 (7), The Consumer Protection Act, 2019.
[14] S. 2 (1) (c), The Commercial Courts Act, 2015.

financial gains. The Act, 2019 does not envisage exclusion of all economic loss from harm to be compensated under product liability actions. A parallel can be drawn from strict liability provisions of the Motor Vehicles Act,[15] where a rich jurisprudence of case law has determined formulas for calculation of loss of life, injury and consequential loss of income, consortium, mental agony etc.[16] In the present case as well, if loss of life or injury leads to long term loss of income or employment, the product manufacturer or seller if found liable should be made to compensate for such economic loss.

At this juncture it would be appropriate to discuss in some detail provisions specifically contained in Chapter VI of the Act, 2019. A perusal of Sections 82 and 83 clearly shows that a consumer complaint disclosing a claim for product liability i.e., a product liability action can be brought against the following three categories of persons:

i. Product Manufacturer
ii. Product Service Provider
iii. Product Seller

1. Defect, Defective Design and Manufacturing Specifications

The definitions of the above-mentioned category of persons discloses that the three terms encompass within them all possible roles such as making/assembling a product, rebranding or marking, selling, distribution, leasing, installing, repairing, maintaining, designing, fabricating etc.[17] However, the Act, 2019 creates three separate categories of instances when either the Product Manufacturer, the Service Provider or the Seller would be liable. Under Section 84 of the Act, liability for a Product Manufacturer is provided in five specific instances as follows:

i. Manufacturing defect;
ii. Defective design;
iii. Deviation from manufacturing specifications;
iv. Violation of express warranty;

[15] S. 140, The Motor Vehicles Act, 1988 (now omitted vide Section 50, The Motor Vehicles (Amendment) Act, 2019).
[16] Sarla Verma (Smt.) v. Delhi Transport Corporation, 2009 (6) SCC 121.
[17] See S. 2(36) and 2(37), The Consumer Protection Act, 2019.

v. Failure to provide adequate instructions or warnings.

In the categories of cases mentioned above, consumer fora have a healthy jurisprudence pertaining to manufacturing defects. However, the terms 'defective in design' and 'manufacturing specifications' contained in the Section warrant some analysis. Design or manufacturing specifications in the Indian context are generally governed only for a limited set of products by special legislations governing such products. The Bureau of Indian Standards Act, the Rules and the Notifications issued thereunder, govern the minimum standard of some products such as cement, electrical appliances, processed foods etc.[18] Similarly the Drugs and Cosmetics Act, the Rules thereunder govern pharmaceutical products.[19] The Consumer Commissions therefore while examining minimum standards to be maintained, and while examining design or manufacturing specifications of goods governed by specific legislation, need to mandatorily borrow definitions and standards laid down by such rules or notifications. Even when the goods are not mandatorily regulated by the special legislation, guidance can be sought from these specific legislations while examining recommended standards or standards for similar goods. The Consumer Commissions also need to be wary of the fact that merely because a product has been manufactured in accordance with the manufacturer's own manufacturing specifications or design would not mean that such product is incapable of causing harm. The reasonableness of such design or specifications has to be examined by examining similar goods or by taking expert assistance in ascertaining whether such specifications or design are proper. It is time that the Consumer Commissions force manufacturers to adhere to the highest possible manufacturing standards and even unhygienic or hazardous manufacturing conditions should be considered as violation of specifications and a manufacturing defect.

2. Instructions and Warnings

Perhaps one of the most important categories of liability of manufacturers is Section 84(1)(e) i.e., when the product fails to contain adequate

[18] The Bureau of Indian Standards Act, 2016.
[19] The Drugs and Cosmetics Act, 1940.

instructions of correct usage to prevent any harm or any warning regarding improper or incorrect usage. Though, for most hazardous goods, specific legislations compulsorily force manufacturers to display instructions and warnings merely because an item is not inherently hazardous to life or property would not mean that a manufacturer would not be liable to examine all possible hazards of such a product and display them. Further, the mandate of proper instructions of usage and display of warnings should not be treated as a mere formality by Consumer Commissions while adjudicating a product liability claim arising out of harm caused as a consequence of such instruction or warning. That is to say, even if there exists no legal mandate to display instructions and warnings in a particular manner, such text and images should be displayed prominently, clearly and without obstruction.

The Consumer Commission should examine such text and images on the basis of reasonable understanding of the final intended consumer or any reasonable user.[20] For instance, a warning/instruction solely in English or Hindi language on an item which is to be used in agricultural or domestic use all over the country would not be sufficient warning, since its intended user can be reasonably assumed to have limited knowledge of only local languages. From experience in more mature product liability jurisdictions such as the USA, it has also become amply clear that a manufacturer ought to foresee possible and reasonable uses and misuses of a product and provide reasonable warning related to such unintended uses.[21] A classic example for such cases is that of a chair, where it is reasonably assumed that a consumer during the course of the product's usage might stand on the chair for support, etc. In such a case if the chair can be hazardous and is incapable of such usage, the manufacturer has a duty to warn the consumer about such misuse and its consequences.

It may be argued by manufacturers that putting such a heavy burden of mandatory warnings and instructions even for unforeseeable risks, for

[20] F.C. Schafrick, *Product Liability suits for failure to warn of the hazards of regulated products,* 32(3) Tort & Insurance Law Journal 833, 837 (1997).
[21] V.E. Schwartz, *Continuing Duty to Warn: An Opportunity for Liability Prevention or Exposure*, 17(1) Journal of Public Policy & Marketing 124, 125 (1998).

products which are inherently not dangerous or hazardous is beyond the intent of product liability provisions under the Act, 2019. However, in the absence of any specific exclusion clause in Section 84 and usage of broad terms such as 'adequate instructions' and 'any warnings' it is amply clear that the legislature intended to place a heavy burden upon the manufacturer. The same is further solidified by jurisprudence and legislations in jurisdictions such as the USA and the UK.[22] It is imperative that the Consumer Commissions recognize the importance of these provisions in self-regulating the marketspace without actual legislative interference in every minute detail of packaging, labeling or marking of the product. It may also be noted that the Central Government has been granted rule making powers under the Act, 2019 to further enable enforcement of its provisions. It would be prudent for the Central government to deliberate upon creating product liability rules to clarify terms aforementioned and lay down minimum standards for unregulated goods. Such an exercise of delegated legislation would sufficiently guide the Consumer Commissions in ensuring the maximum effect of product liability provisions under the Act.

3. Product Service Provider and Seller

A product service provider under the Act, 2019 is defined to mean any person who provides a service in respect of any product.[23] This definition has been added specifically to deal with services such as maintenance or repair services where the service and product are inherently related and the service has a direct consequence upon the performance of the product. Needless to state, a deficient service provided by a product service provider can render the product defective/damaged thereby causing harm to the consumer. It is for this reason that Chapter VI of the Act specifically deals with liability of a product service provider in certain specific instances.[24] These instances are similar to liability of a manufacturer under Section 84 and are focused upon the service element of the harm caused by the

[22] J. J. Argo & K. J. Main, *Meta-Analyses of the Effectiveness of Warning Labels,* 23(2) Journal of Public Policy & Marketing 193, 205 (2004).
[23] S. 2 (38), The Consumer Protection Act, 2019.
[24] S. 85, The Consumer Protection Act, 2019.

product. The product service provider therefore has a clear onus of providing good quality services while disclosing all information, instructions and warnings.

A product service provider may be exclusively liable if harm is caused due to an incident triggered by deficiency in services that render the original product defective. In cases involving deficient product services such as repair or maintenance, a consumer while filing a complaint would in most cases implead both the manufacturer and the product service provider as parties to the dispute, since as a consumer the complainant cannot be assumed to possess expert knowledge as to whether the harm has been caused due to a defective product or a deficient product service. In such cases, Consumer Commissions should not hesitate in granting compensation to a complainant if the liability cannot be pinpointed on either the manufacturer or service provider. In such cases both the manufacturer and service provider should be considered jointly liable to provide compensation to the complainant if the evidence suggests that harm has been caused by a product deficiency, though not strictly attributable to one of the parties. The Consumer Commissions should also in such joint liability cases, avoid scientifically distributing the liability in the final decree. The aforementioned examination would obviously be subject to the fact that such product service should not be in violation of warranty conditions i.e., in an unauthorized manner. If such unauthorized service leads to harm from a product, reasonably the manufacturer should not be held liable.

The Act, 2019 has proactively included within the fold of product liability actions not just a product manufacturer or product service provider but also a product seller. Liability of a product seller however, is attracted only in specific conditions enumerated in the Act.[25] The basis of this liability is control over the product. Accordingly, if a product seller has control over designing, testing, manufacturing or labelling of a product or has altered or modified the product, then product liability claims are maintainable against the product seller. Additionally, if the product seller has exercised any

[25] S. 86, The Consumer Protection Act, 2019.

control in assembling or maintaining the product, or gives any warranty in excess of the manufacturer's warranty, he can be liable under the Act, 2019 for any consequent harm caused. The two most important elements of this provision however, are:

i. Vicarious liability under Section 86(d)
ii. Failure to warn under Section 86(e)

Liability under Section 86(d) is being categorized as vicarious because under this sub-section no immediate fault, negligence or control is attributable to the product seller and merely by virtue of sale of the product, liability can be attracted in the following instances:

i. Identity of product manufacturer is not known,
ii. Service of notice or process cannot be affected on product manufacturer
iii. Manufacturer is not subject to the law which is in force in India
iv. Order if passed cannot be enforced against him.

This Section therefore imposes a strict no-fault liability upon a product seller if any of the aforementioned conditions are fulfilled. This nature of liability becomes extremely important in cases involving online intermediaries and e-commerce platforms. Furthermore, in cases involving sale of imported goods, the onus of ensuring quality of goods is squarely placed upon the person selling such goods since if the manufacturer does not have offices in India, according to this section, the entire liability of any harm arising out of such goods would lie upon the product seller in India. The aggrieved consumer would also not be deprived of compensation if the product manufacturer evades service of summons/court process issued by the Consumer Commissions and in such cases the product seller would be liable to compensate the consumer in product liability action. Though this provision is extremely consumer friendly and is oriented towards ensuring that rights of a consumer are not hampered by virtue of non-existence or non-responsiveness of a manufacturer; the Commissions should be extremely cautious in not summarily allowing manufacturers to evade service in each product liability case and thereby forcing product sellers to incur such liability. If the Commissions tacitly become parties to such evasion by the manufacturers,

the regulatory purpose of the product liability provisions would be defeated and it would not effectively deter marketspaces to become more equitable.

Section 86(e) of the Act, 2019 rightly and proactively puts a heavy burden of conveying relevant information, instruction and warning with regard to any product to the consumer. If it is proven in a product liability action that the proximate cause of harm is failure to convey such information or warning, the product seller would also be rendered liable. Such duty to warn is regularly administered in the domain of drugs and cosmetics where only a registered pharmacist is allowed to sell pharmaceutical products while clearly conveying all information and warning to the consumers. Introduction of this positive duty in all consumer goods, is a monumental step in ensuring a more transparent and safer marketspace. It is therefore imperative upon the Ministry of Consumer Affairs to develop information modules and marketing material to inform all product sellers including online marketspaces, individual retailers etc. about the nature of basic information to be shared with consumers while selling different categories of goods. It would be prudent for the central government to enact specific rules highlighting categories of goods, relevant information, warnings etc. to guide the marketspace more efficiently. A case-to-case analysis in each dispute which arises; of whether what nature of information should have been conveyed by a seller to an aggrieved consumer would render the scheme of this section liable to vague outcomes.

IV. CLASS ACTION OR THE CENTRAL CONSUMER PROTECTION AUTHORITY?

One of the primary arsenals of courts in the USA for regulating marketspaces is class action suits arising out of product liability claims. These behemoth cases, if successful, can have financial ramifications affecting the entire business operations of companies. Courts in the USA have therefore converted *inter se* disputes between consumers and manufacturers/service providers as a tool of *in rem* regulation of market behavior.[26] There are of course abundant safeguards in place to ensure that

[26] See S. Acker, *Improving Your Response to Product Liability Claims*, 105 SAE Transactions 220, 228 (1996). Product liability claims have forced manufacturers to develop methods

these litigations are fair and transparent for both parties. In the Indian context unfortunately, though the Act, 1986 allowed for a class of consumers to file consumer complaints for common causes of action; class action or similar large-scale litigation never gained significance like its American counterparts. This was primarily a result of narrow interpretations given by consumer fora and reluctance in granting punitive damages which would have any deterrent value. A consumer dispute in India therefore *prima facie* remains an *inter se* dispute between one consumer and one manufacturer/service provider and compensation is awarded more or less considering the retail price of the product/service vis-a-vis inconvenience or loss caused. The paying capacity of the manufacturer/service provider and the overall ramification of the product to the public at large is not considered as a relevant fact and hence, exemplary or punitive damages are seldom awarded.

The situation under the Act, 2019 more or less remains the same as far as adjudication of consumer complaints is concerned. However, if the same reasoning is extended to product liability claims, then a manufacturer can potentially introduce hazardous, dangerous goods with a calculated risk of potential claims if and when filed. Since these claims would arise in their own respective silos of territorial jurisdiction etc., the financial ramification of these claims would not be sufficient to deter the manufacturer from introducing these goods in the future or withdrawing hazardous goods. Additionally, due to a low-cost conundrum, most low retail price goods which cause harm to consumers would go unassailed before the Consumer Commissions since it would not make financial sense for a single consumer to file consumer complaints for such consideration or minor harm.[27]

One solution to this problem is of course training of Consumer Commissions to ensure that the complaints filed by multiple consumers on common cause of action related to product liability may be dealt with strictly while considering the potential harm of such product on the entire

to document product development, specifications and ascertain all possible hazards in usage of the product.

[27] V. K. Singh & A. K. Singh, *Central Consumer Protection Authority - A Critical Analysis*, 8 International Journal on Consumer Law and Practice 59, 65 (2020).

marketspace. Consumer Commissions must exercise powers of awarding punitive damages in such appropriate cases and punitive damages must be calculated on the basis of the potential harm caused to public at large and approximate profit earned by sale of such defective product/service.[28] Further, the Commissions must be proactive in issuing injunctive relief such as withdrawing goods from sale, cease manufacture and sale of hazardous goods etc.[29]

However, this still leaves two potential lacunae, firstly, Consumer Commissions are primarily adjudicatory bodies *in personam* and do not exercise jurisdiction *in rem;* and secondly, Consumer Commissions have no powers of *suo motu* exercise of jurisdiction and must wait for actual harm to be caused for exercise of its powers. It is in these circumstances that the newly created Central Consumer Protection Authority (**"CCPA"**) becomes extremely relevant. The CCPA is a regulatory authority created under the Act, 2019 with powers of investigation, inquiry and injunctive actions.[30] The CCPA can exercise *suo motu* jurisdiction in cases involving violation of consumer rights where such violation is prejudicial to the public interest or to the interests of consumers as a class.[31] In product liability actions which may come to the attention of the CCPA whether filed before the Commissions or through public/social media; the CCPA can initiate *suo motu* preliminary inquiry into such alleged potentially harmful goods. If the preliminary inquiry discloses violation of consumer rights such as hazardous goods/services, absence of instructions/warnings, false warranties etc.; detailed investigation can be initiated by the CCPA's investigative wing.[32] Such investigation can include search and seizure, discovery of documents and recording of evidence upon issuing show cause notices to the manufacturer/product service provider. Thus, even before filing of a complaint after actual harm has occurred, the CCPA can *suo motu* regulate the market after following due process of law. If such

[28] See Liebeck v. McDonald's Restaurants, 1995 WL 360309 (1995, District Court of New Mexico). Punitive damages were calculated on the basis of daily profit of McDonald's Restaurants. Similar provision exists in S. 39, The Consumer Protection Act, 2019.
[29] Power to grant injunctive relief is inherent under S. 39 (1), The Consumer Protection Act, 2019.
[30] Chapter III, The Consumer Protection Act, 2019.
[31] S. 18 (2) (a), The Consumer Protection Act, 2019.
[32] S. 19 (2), The Consumer Protection Act, 2019.

investigation reveals harm caused to large number of consumers, the CCPA can direct a product manufacturer or product service provider to provide reimbursement, compensation, recall and repair goods, prohibition on sale of goods to each and every consumer who had purchased such a product or availed such a product service.[33] The heavy burden of adducing evidence by each affected consumer would be satisfied by the investigative powers of the CCPA.

V. CONCLUSION

The provisions related to product liability actions as introduced by Chapter VI of the Act, 2019 and supplemented by the definition section are undoubtedly a derivation from more mature product liability regimes such as the USA. Though some experiences from such jurisdictions can act as guiding principles to Indian tribunals as discussed in this paper, given the differences in social, economic and judicial systems between India and other jurisdictions, Consumer Commissions need to implement product liability provisions with extreme caution and while balancing the intent of the Act, interest of the consumer and of the marketplace. The Consumer Commissions also need to ignore specific jurisprudence under the Act, 1986 so as not to get restricted by judicial pronouncements which were delivered in a different legislative framework and socio-economic background. With a growing economy and ever-increasing profit margins of manufacturers, sellers, service providers and online marketplaces; it is the duty of the Consumer Commissions to ensure a more equitable and transparent market for a common consumer.

If implemented in a just, fair and reasonable manner, product liability regime as has been introduced by the Act, 2019 has the potential of not only ensuring just compensation and restitution to aggrieved consumers but to also regulate manufacturers, product service providers and product sellers without resorting to excess regulation by legislative intervention into every element of commerce and trade.

[33] S. 20, The Consumer Protection Act, 2019.

UNDERSTANDING HARM FROM PERSONAL DATA PROCESSING ACTIVITIES AND ITS CHALLENGES FOR USER PROTECTION

[*]Srikara Prasad

ABSTRACT

This article seeks to understand the nature of harm emerging from personal data processing activities and its impact on user protection. To this end, the article analyses how personal data-related harms are unique and distinct from other kinds of harms arising from torts, breach of contract, crime or defects in products and services. Then, it explores how these unique features of personal data-related harm could pose practical challenges to existing and upcoming frameworks for user protection and redress in relation to personal data. In doing so, the article analyses how the treatment of 'Harm' under the Personal Data Protection Bill, 2019 risks weakening user protection measures in the Bill. Finally, the article uses the analysis to justify an alternative definition for 'Harm' that would allow future jurisprudence to develop on a case-by-case basis until there is a firmer understanding of how to address the challenges posed by personal data-related harms.

I. INTRODUCTION

The digital economy in India has seen tremendous increase in the user[1] activity over the past few years. A wide bouquet of services, including essential services like finance and social security schemes, are now being delivered digitally. This has made many services accessible and convenient for users. For example, mobile banking is allowing users to make banking transactions from their homes, reducing their reliance on physical bank

[*] Srikara Prasad, Policy Analyst, Future of Finance Initiative at Dvara Research. He was assisted by Ms. Hussanpreet Kaur, II Year Student, Rajiv Gandhi National University of Law, Punjab.

[1] The word 'Consumer' is useful when referring to persons who transact with service providers for commercial purposes. This is different from 'Citizen' who transacts with service providers for social benefits, such as those under various Direct Benefit Transfer schemes. It would be inappropriate to conflate 'Consumers' and 'Citizens' because both have a different set of rights and remedies under the law. This paper will use the word 'User' to refer to both, consumers and citizens who participate in the digital economy for various reasons.

branches in their vicinity. But more importantly, the digital economy has redefined the role of users' personal data in user well-being.

Users generate vast amounts of personal data in the digital economy. This data can help providers understand user preferences better and design products and services better suited to the users' benefit. On the flipside, the mishandling of personal data can be detrimental to users' interests and their right to privacy.[2] The different kinds of risks and harms[3] that arise for users from personal data processing activities and personal data breaches (that this paper addresses as "**personal data-related harm**") can be very difficult to identify and predict.[4] Personal data-related harm, in this sense, is unique and distinct from the general understanding of harm arising from torts, breach of contract, crime or defects in products and services. This unique nature of personal data-related harm could pose difficult practical challenges to user protection under existing and upcoming personal data-related frameworks in India.

Following the Supreme Court's landmark judgment on the right to privacy in *Justice K.S. Puttaswamy v. Union of India*,[5] the Central Government set out to enact a personal data protection law. The ensuing draft of the Personal Data Protection Bill, 2019 ("**the Bill**") seeks to create an elaborate framework to regulate personal data processing[6] activities in India and protect users' interests from harm *ex ante* i.e. preventing harm before it can occur instead of seeking to remedy harm after it occurs.[7] However, one of the most concerning features of this framework is its definition of 'Harm'.[8] The definition prescribes a list of ten outcomes that must be treated as

---

[2] S. Prasad, *Defining 'Harm' in the digital ecosystem*, Dvara Research, available at https://www.dvara.com/blog/2019/05/06/defining-harm-in-the-digital-ecosystem/, last seen on 29/11/2020.

[3] The article uses 'Harm' to refer to harm as defined in the Personal Data Protection Bill, 2019. The word 'Harm' is used for all other purposes.

[4] Supra 2.

[5] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[6] This article relies on the definition of 'Processing' under the draft Personal Data Protection Bill, 2019 that defines 'Processing' under S. 3 (31) as: *"an operation or set of operations performed on personal data, and may include operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction."*

[7] Preamble, The Personal Data Protection Bill, 2019 (pending).

[8] S. 3 (20), The Personal Data Protection Bill, 2019 (pending).

harm from personal data processing activities. The definition does not consider the unique nature of personal data-related harm and risks creating practical challenges for user protection and redress in the Bill. These challenges could also arise under other user protection frameworks relating to personal data in India including common law, the Code of Civil Procedure, 1908 ("**the CPC**"), the Information Technology Act, 2000 ("**IT Act**") and the Consumer Protection Act, 2019 ("**the CPA**").

In this context, it is important to understand what makes personal data-related harm unique and what practical challenges they pose for user protection. This article first provides an overview of the role that personal data plays in the digital economy and the benefits and risks that ensue for users (Section 2). Then, it discusses how personal data-related harm is unlike other kinds of harm (Section 3). This is followed by an analysis of the practical challenges that the uniqueness of personal data-related harm creates for user protection under existing and upcoming user protection and redress frameworks (Section 4). Lastly, the article uses this analysis to justify the need for and propose an alternative definition of 'Harm' that would be more suitable for user protection in data processing activities (Section 5).

II. THE ROLE OF PERSONAL DATA IN THE DIGITAL ECONOMY: BENEFITS & RISKS TO USERS

1. Benefits to Users

Users share a lot of personal data when they participate in the digital economy.[9] For example, a user, who creates a profile on a social media platform, shares his name, date of birth, address, E-Mail addresses, preferences, etc. when they sign up. Users further generate personal information when they engage with content on the social media platform signaling what they like, what content they view, who they befriend, etc. Similarly, a user who makes digital financial transactions (like payments)

[9] *The value and role of data in electronic commerce and the digital economy and its implications for inclusive trade and development note by the UNCTAD Secretariat*, U.N. Document TD/B/EDE/3/2, available at https://unctad.org/system/files/official-document/tdb_ede3d2_en.pdf, last seen on 04/12/2020.

has to share his personal information like their Permanent Account Number ("**PAN**") number, Aadhaar number and biometric identifiers to fulfill the financial institution's Know-Your-Customer ("**KYC**") requirements.[10]

Users further generate personal information when they make transactions signaling what they buy, how often they buy etc. Users generate vast amounts of personal data through their activities in the digital economy, some of which (such as health data and financial data) could be highly sensitive in this manner.[11] Developments in data processing techniques and abilities have enabled providers to process these vast amounts of personal data popularly known as big data analytics, and glean valuable insights about users.[12] Providers can use these insights and create products and services that can better match users' preferences. For instance, a food delivery platform could process a user's food order history on the platform to learn their preferences and curate a bespoke list of restaurants for that user.[13] On a larger scale, providers could aggregate users' personal data from different sources to create an aggregated dataset and generate a digital profile that can help in the delivery of services.[14] For example, financial institutions can use such aggregated datasets to create a user's psychometric profile and assess the user's credibility before sanctioning a loan.[15]

---

[10] *Know Your Customer (KYC) Direction, 2016*, RBI Master Direction No. DBR.AML.BC.No.81/14.01.001/2015-16 (25/02/2016), available at https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD18KYCF6E92C82E1E1419D87323E3869BC9F13.PDF, last seen on 04/10/2020.

[11] Ministry of Electronics and Information Technology, Government of India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, available at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, last seen on 30/11/2020.

[12] *Big Data in Action for Government*, World Bank Group, available at https://openknowledge.worldbank.org/bitstream/handle/10986/26391/114011-BRI-3-4-2017-11-49-44-WGSBigDataGovernmentFinal.pdf?sequence=1&isAllowed=y, last seen on 04/12/2020.

[13] E. Knight, *It's the Algorithm, It Decides: An Autoethnographic Exploration of Algorithmic Systems of Management in On-Demand Food Delivery Work in Amsterdam*, available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjQx-bR9LTtAhVIzTgGHep_DekQFjAAegQIAxAC&url=https%3A%2F%2Fscripties.uba.uva.nl%2Fdocument%2F674434&usg=AOvVaw1ZpDVb47Ybf_WU7UgFiaio, last seen on 04/12/2020.

[14] *Examples of Data Points Used in Profiling*, Privacy International, available at https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf, last seen on 04/12/2020.

[15] Financial institutions rely on a person's credit reports and credit score to assess a person's creditworthiness i.e., their eligibility for a loan. Traditionally, credit reports are

Providers can harness users' personal data towards users' welfare in this manner.

2. Risks and Harm to Users

On the flipside, the use of personal data can expose users to the risk of harm.[16] It is well-established that a variety of harms can emerge when personal data is breached, misused or processed improperly;[17] ranging from mental agony to financial loss, discrimination, surveillance and user manipulation.[18] These harms can be amplified forms of existing and known harms or be newer and inchoate forms of harm (like user manipulation)[19] that emerge with developments in technology and use-cases for personal data.[20] Personal data-related harms could be categorized into two broad categories: primary harms and secondary harms.[21] Primary harms emerge when personal data is breached. It refers to the immediate outcomes of a

based on a person's credit history– previous loans sanctioned, repayment history, defaults etc. However, emerging practices are using different kinds of data including a person's utility bill payments, mobile phone activity etc. to assess the person's creditworthiness. See, A. Singh & S. Prasad, *Artificial Intelligence in Digital Credit in India*, Dvara Research, available at https://www.dvara.com/blog/2020/04/13/artificial-intelligence-in-digital-credit-in-india/, last seen on 22/11/2020. Also see, *High Level Task Force on Public Credit Registry*, Report of the High Level Task Force on Public Credit Registry, available at https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=895, last seen on 1/12/2020.

[16] Supra 11.

[17] Supra 2; B. Chugh & N. Kumar, *Harms to Consumers in a Modular Financial System*, Dvara Research, available at https://www.dvara.com/blog/2017/11/07/harms-to-consumers-in-a-modular-financial-system/ , last seen on 24/11/2020; R. Calo, *The Boundaries of Privacy Harm*, 86(113), Indiana Law Journal 1131, 1142-1156 (2011), available at http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf, last seen on 29/11/20.

[18] Supra 2.

[19] For example, the Cambridge Analytica incident showed how users' personal data could be used to understand and manipulate users' mental models. Insights derived on users seem to have helped in manipulating user preferences and behaviours across the world, including in India. See Cambridge Analytics: The data firm's global influence, BBC, available at https://www.bbc.com/news/world-43476762, last seen on 29/11/2020.

[20] Supra 2.

[21] Ibid.

personal data breach such as privacy infringement,[22] financial loss,[23] harassment,[24] etc.[25] Secondary harms arise when personal data, breached or otherwise, is processed.[26] These harms are a result of processing activity

[22] For example, big data techniques have enabled curation of large, aggregated datasets that can provide a birds-eye view on different groups of users. A breach of any one user's personal data in these datasets' risks infringing the privacy of all other similar users in the dataset collectively. See, B. Chugh & N. Kumar, *Harms to Consumers in a Modular Financial System*, Dvara Research, available at https://www.dvara.com/blog/2017/11/07/harms-to-consumers-in-a-modular-financial-system/, last seen on 24/11/2020. Also see, L. Taylor, L. Floridi & B. van der Sloot, *Safety in Numbers? Group privacy and Big Data Analytics in the Developing World, 24, in Group Privacy: New Challenges of Data Technologies* (Taylor, L. Floridi & B. van der Sloot, eds. 2017). Further, providers' abilities to process user activity and glean insights could also infringe users' privacy. For instance, in 2012, a New York Times report revealed how Target would analyses users' purchases and understand if the user is pregnant. See, C. Duhigg, *How Companies Learn Your Secrets*, New York Times, available at https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp, last seen on 29/11/2020.

[23] A breach of sensitive datasets, such as those containing account credentials or biometric information, could similarly make users vulnerable to phishing, fraud etc. For example, see *Timeline of Cyber Incidents Involving Financial Institutions,* Carnegie Endowment for International Peace, available at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline, last seen on 28/11/2020.

[24] For example, certain digital lending mobile applications access users' personal data on the mobile phone such as contacts, photos etc. as collateral for credit (sometimes without providing due notice to the user). Reports suggest that at the time of loan recovery, the lenders have threatened to leak sensitive images, or have contacted users' social and professional circles to name and shame the user. See, S. Ghosh, *App Lenders Scar Young Debtors*, Livemint, available at https://www.livemint.com/companies/news/app-lenders-scar-young-debtors-11600132261735.html, last seen on 29/11/2020. Also see, P. Mallikarjunan, *How App-Based Lenders are Harassing, Sucking Borrowers Dry*, Moneylife, available at https://www.moneylife.in/article/how-app-based-lenders-are-harassing-sucking-borrowers-dry/60621.html, last seen on 29/11/2020; and D. Sharma, *Shocking Tactics of Lenders Exposed! Loan Recovery Agents Blackmailing Customers After Hacking Phones*, Mid-day, available at https://www.mid-day.com/articles/shocking-tactics-of-lenders-exposed-loan-recovery-agents-blackmailing-customers-after-hacking-phones/22896205, last seen on 29/11/2020.

[25] K. Kemp, *Big Data, Financial Inclusion and Privacy for the Poor*, Dvara Research, available at https://www.dvara.com/blog/2017/08/22/big-data-financial-inclusion-and-privacy-for-the-poor/, last seen on 29/11/2020.

[26] Supra 2.

and can include identity theft,[27] discrimination,[28] exclusion,[29] inaccurate profiling and surveillance.[30]

Personal data-related harms can also be tangible or visceral. Seminal literature on harm related to privacy and personal data by Ryan Calo (2011) classifies harms into two categories: subjective harms and objective harms.[31] Subjective harms refer to harms that are "internal to the person harmed". They refer to "unwelcome mental states" such as anxiety, embarrassment and fear that a user may experience due to unwanted observation. Objective harms refer to harms that are "external to the person harmed". They stem from the "unanticipated or coerced use of information concerning a person against that person" that result in an external effect such as financial loss. It is important to note that these categories are not watertight. Subjective harms could arise due to the

[27] The advent of DeepFakes i.e., highly realistic media synthesized by processing visual or audio data on users using artificial intelligence systems creates a new frontier for identity theft. There have already been instances where DeepFakes have made people vulnerable to extortion and blackmail. See, D.K. Citron & R. Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 California Law Review 1753, 1772 (2019), available at https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship, last seen on 24/11/2020.

[28] For example, an investigative report published in April 2016 showed that Amazon, Inc's Prime Free Same-Day deliveries service excluded areas in cities which were predominantly occupied by the African American community. See D. Ingold & S. Soper, *Amazon Doesn't Consider the Race of Its Customers. Should it?* Bloomberg, available at https://www.bloomberg.com/graphics/2016-amazon-same-day/, last seen on 28/11/2020. More recently, Apple, Inc's credit card algorithm sanctioned different amounts of credit for men and women, offering smaller credit amounts to women. See, W. Knight, *The Apple Card Didn't 'See' Gender – and That's the Problem*, Wired, available at https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/, last seen on 28/11/2020.

[29] For example, many public services are increasingly being delivered digitally based on users' Aadhaar numbers. However, data quality issues in the Aadhaar database (such as spelling mistakes in names, biometric mismatches etc.) have led to users being unable to access public services. See, R. Khera, *Aadhaar Failures: A Tragedy of Errors*, EPW Engage, accessible at https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare, last seen on 28/11/2020.

[30] Supra 25; D.J. Solove, *A Taxonomy of Privacy*, 154(3) University of Pennsylvania Law Review 477, 491-553 (2006), available at https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf, last seen on 29/11/2020; B. Chugh & N. Kumar, *Harms to Consumers in a Modular Financial System*, Dvara Research, available at https://www.dvara.com/blog/2017/11/07/harms-to-consumers-in-a-modular-financial-system/, last seen on 24/11/2020; L. Taylor, L. Floridi & B. Van Der Sloot, *Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World, 24, in Group Privacy: New Challenges of data technologies* (Taylor, L. Floridi & B. van der Sloot, eds. 2017).

[31] R. Calo, *The Boundaries of Privacy Harm*, 86(113), Indiana Law Journal 1131, 1142-1156 (2011), available at http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf, last seen on 29/11/20.

perceived risk of objective harms emerging from personal data. However, this distinction is useful in understanding the different dimensions of personal data-related harms: one dimension which is purely internal to a user and another that is external. While objective harms would be visible and objectively verifiable, subjective harms would be visceral and difficult to verify.

Harm is usually understood to be a setback to a person's interests.[32] However, the unique nature of personal data-related harms makes it difficult to identify setbacks to users' interests. The following section analyses how harms relating to personal data are unique and distinct from other kinds of harm.

III. THE UNIQUENESS OF PERSONAL DATA-RELATED HARMS

Although it is clear that mishandling personal data can lead to harm, it is very difficult to understand 'how' and 'when' harm will occur.[33] For instance, once personal data is breached, it is extremely difficult to identify who has access to the personal data, understand what it might be used for or predict when it might be used. The entities breaching personal data could process personal data for themselves or share it with other entities. They could process personal data that they obtained from a breach or they could process personal data after aggregating different datasets obtained from other sources. The entities could process the personal data immediately after the breach or after many weeks, months or years. A similar problem exists in relation to cases of improper processing of personal data. As seen in the case of the Apple Card where the credit decisioning algorithm inconceivably discriminated against female users,[34]

---

[32] S. Perry, *Harm, History, and Counterfactuals*, 40, San Diego Law Review, 1283, 1284-1285 (2003), available at https://www.law.upenn.edu/cf/faculty/sperry/workingpapers/B40SanDiegoLR1283(2003).pdf, last seen on 04/12/2020; D.J. Solove & D. Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, GWU Law School Public Law Research Paper No. 2017-2, 6-7, GWU Law School Public Law Research Paper No. 2017-2 (2017), available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2499&context=faculty_publications, last seen on 04/12/2020.

[33] Supra 2.

[34] W. Knight, *The Apple Card Didn't 'See' Gender – and That's the Problem*, Wired, available at https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/, last seen on 28/11/2020.

even *bona fide* processing of personal data could eventually have a *mala fide* impact on the users. In this sense, harms that can arise once personal data is processed or breached can neither be identified nor be predicted with certainty, making them indiscernible and unpredictable.[35] Therefore, a user, provider or a regulator might not even know if a breach of a processing activity has caused a setback to users' interests.

Harms arising from torts, breach of contract, crime, deficiencies in products and services etc., are comparatively a lot simpler to identify and predict. For instance, consumer protection laws have benefited from the reasonable certainty about what is "harmful" for consumers. The Consumer Protection Act, 2019 ("**CPA**") defines harm under S. 2(22):

> 'Harm', in relation to product liability, includes –
> *(i)* damage to any property, other than the product itself;
> *(ii)* personal injury, illness or death;
> *(iii)* mental agony or emotional distress attendant to personal injury or illness or damage to property; or
> *(iv)* any loss of consortium or services or other loss resulting from a harm referred to in sub-clause (i) or sub-clause (ii) or sub-clause (iii), but shall not include any harm caused to a product itself or any damage to the property on account of breach of warranty conditions or any commercial or economic loss, including any direct, incidental or consequential loss thereto;

This definition prescribes what 'Harm' is, based on consumer outcomes emerging from defects[36] and deficiencies[37] in products and services, misleading advertisements,[38] restrictive trade practices[39] and unfair trade practices (which are central to the consumer protection framework in the CPA).[40] Having such a clear and precise definition of 'Harm' allows stakeholders to identify harm with certainty and allows consumers to ask for redress on clear and justifiable grounds. However, the indiscernibility and unpredictability of personal data-related harms makes it impossible to define what harm is, in personal data processing activities. This problem is apparent in the draft Bill, which by attempting to prescribe a specific

[35] Supra 2.
[36] "Defect" is defined under S. 2 (10) of the Consumer Protection Act, 2019.
[37] Ibid, S. 2(11).
[38] Ibid, S. 2(28).
[39] Ibid, S. 2(41).
[40] Ibid, S. 2(47).

definition for 'Harm',[41] creates a definition that is extremely broad, vague and difficult to interpret.

The Bill defines 'Harm' under S. 3(20):

> "'Harm' includes –
> *(i)* bodily or mental injury;
> *(ii)* loss, distortion or theft of identity;
> *(iii)* financial loss or loss of property;
> *(iv)* loss of reputation or humiliation;
> *(v)* loss of employment;
> *(vi)* any discriminatory treatment;
> *(vii)* any subjection to blackmail or extortion;
> *(viii)* any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principle;
> *(ix)* any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or
> *(x)* any observation or surveillance that is not reasonably expected by the data principal;"

This provision provides a list-based definition of 'Harm'. The definition provides ten outcomes that would constitute 'harm' under the Bill's framework. The use of the word 'includes' also suggests that this is an inclusive and non-exhaustive definition that could be expanded further based on the rule of *ejusdem generis* (meaning "of the same kind" in Latin) in statutory interpretation.[42] The *ejusdem generis* rule is helpful in interpreting definitions that contain a set of items. The rule allows expanding a list of items in a definition to include other items if they are of the same kind.[43] For instance, if a provision defines a term as "including, apples, mangoes, pineapples and banana", the provision could be expanded to include other fruits like guava and watermelon. The rule relies on a common thread running through a provision to provide guidance in identifying similar items that can be added to the scope of the provision (and dissimilar items that cannot).

[41] Supra 8.
[42] Ejusdem generis, Legal Information Institute, available at https://www.law.cornell.edu/wex/ejusdem_generis, last seen on 04/12/2020.
[43] Ibid.

Analyzing the Bill's definition of 'Harm' through this lens shows that the definition lacks a common thread passing through the ten outcomes.[44] The definition seems to include (i) all kinds of physical, mental and emotional injury (ii) all kinds of injury to property and reputation (iii) all kinds of interference with constitutional rights and (iv) other distinct outcomes that are not strictly covered by any of the other categories of outcomes. There is no guidance in the provision about how to include and exclude new outcomes into the list in the definition under the rule of *ejusdem generis*. The scope of the definition is extremely wide and could cover almost any outcome and treat it as harm under the Bill.[45] Therefore, in attempting to list all the potential harms that could emanate from the processing of personal data, the Bill creates a very vague and open-ended definition that is very difficult to interpret.[46] As a result, the challenges in identifying harm remain unaddressed.

Further, high amounts of information asymmetry between users and providers (who process personal data) intensifies the problem of identifying personal data-related harms. Millions of users generate many exabytes of personal data that is processed by thousands of entities in a digital economy. However, users rarely have an understanding of the entities which have their personal data and what it is being processed for.[47] This information asymmetry is sharpened by data breaches which cast shadows over how personal data flows in the economy. When harm materializes in this context, the information gaps could make it close to impossible for users to demonstrate a causal link between the harm and a breach or personal data processing activity by a particular entity.[48]

---

[44] S. Prasad, *An Analysis of 'Harm' defined under the draft Personal Data Protection Bill, 2018*, Dvara Research, available at https://www.dvara.com/blog/2019/10/29/an-analysis-of-harm-defined-under-the-draft-personal-data-protection-bill-2018/, last seen on 29/11/2020.

[45] Ibid.

[46] Supra 44.

[47] Supra 11.

[48] *See* D.J. Solove & D. Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, GWU Law School Public Law Research Paper No. 2017-2, 1, GWU Law School Public Law Research Paper No. 2017-2, George Washington University Law School, (2017), available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2499&context=faculty_publications, last seen on 04/12/2020.

These challenges with personal data-related harms: indiscernibility, unpredictability and the difficulty in demonstrating causation, make them unique and distinct from other kinds of harm and from the general understanding of harm. The following section discusses the challenges that could arise for user protection and redress, given these characteristics of personal data-related harms.

IV. PERSONAL DATA-RELATED HARM: CHALLENGES TO USER PROTECTION AND REDRESS IN INDIA

The unique characteristics of personal data-related harm create some practical challenges for user protection and redress in India. This section first introduces the existing frameworks for user protection and redress in India in relation to personal data, and then analyses the challenges they face due to personal data-related harms. Then, it introduces the upcoming framework for user protection and redress under the Bill and analyses how personal data-related harm could challenge this framework. In doing so, the section explores how existing and upcoming frameworks could be inadequate or unsuitable for protecting users and providing redress in personal data-related harms.

1. Challenges for User Protection and Redress Under Existing Personal Data Protection Frameworks: India

The prominent legal frameworks in force today that are applicable to user protection in data processing activities include:

i. Torts and common law: Under common law, aggrieved users can approach the court seeking redress when they suffer injury due to an act, omission or negligence of another person or entity.[49]

ii. The IT Act, 2000: Providers (termed as "Body corporates" in the Act) can be held liable for negligence if they do not adopt reasonable security practices and as a result lead to a wrongful loss

[49] Smt. Anguri v. Jiwan Dass, (1988) 4 SCC 189.

to users. Such providers are liable to compensate users for the wrongful loss suffered.[50]

iii. The CPA, 2019: The CPA protects consumers against unfair trade practices[51], which include unlawful disclosure of personal data.[52]

iv. The CPC, 1908: The CPC prescribes procedures for users seeking redress in civil cases before civil courts. Such cases would include breach of contracts, including privacy agreements between providers and users, which define the standard of care that providers owe to users with respect to their personal data.

These frameworks do not regulate personal data processing activities. They provide users redress in cases where users suffer personal data-related harms. Users must fulfil two preconditions before they can obtain redress under these frameworks. It is an established common law principle that aggrieved users (plaintiffs) must be able to prove the cause of action and an injury in order to obtain redress.[53] Injuries must be caused by an act or omission of another person or entity. A "cause of action" establishes a causal link between an act or omission and an injury. A plaintiff's claim is actionable only when they can establish a cause of action. However, the causal link should not be remote. The plaintiff should be able to establish to a reasonable degree that the act or omission led to the injury.[54]

Injury is defined as a legal damage, or an interference with a legal right or damage arising from breach of a legal duty. This would include physical injuries, mental injuries, damage to property, damage to reputation, infringement of other legal rights etc. Other kinds of damage, where there is no interference with rights or breach of legal duties, are not actionable.[55]

[50] S. 43A, The Information Technology Act, 2000.
[51] 'Unfair trade practice' is defined under s.2(47) of the Consumer Protection Act, 2019.
[52] S.2 (47), The Consumer Protection Act, 2019.
[53] Alston v. Marine and Trade Insurance Company Ltd. [1964] 4 SA 112 (Witwatersrand Local Division of High Court of South Africa).
[54] Haynes v. Harwood (1935) 1 KB 146 (1935, Court of Appeal of England and Wales); Overseas Tankship (UK) Ltd v. Morts Dock and Engg. Co. Ltd, (1961) AC 388 (1961, Judicial Committee of the Privy Council).
[55] Bhim Singh v. State of J&K (1985) 4 SCC 677.

Similarly, under the CPC, plaintiffs must be able to establish the facts demonstrating a cause of action and an injury.[56] Under the CPA, complainants[57] must be able to establish defects and deficiencies in goods and services, unfair contractual terms and unfair trade practices that cause an injury when they make a complaint seeking relief.[58] Under the IT Act, plaintiffs must be able to establish that Body Corporates did not adopt reasonable security practices because of which they suffered wrongful loss.[59]

Personal data-related harms pose two broad challenges to user protection and redress under these frameworks.

1.1. Users Could Find it Difficult to Establish a Cause of Action

The first challenge that arises is users being unable to establish a cause of action and prove that injury was a consequence of a breach of processing activity. Admittedly, under common law, plaintiffs can hold defendants liable for negligence (misfeasance) and for not providing (nonfeasance) the standard of care that they owe to plaintiffs.[60] This is also embodied under S. 43A of the IT Act. In the context of personal data processing, users may be able to convincingly argue that providers were negligent and failed to provide the standard of care required in adopting necessary security measures to protect personal data from breaches.

However, it would be difficult for users to make this argument for secondary harms emerging after a data breach. Under established principles of common law, defendants would not be liable for consequences that were too remote from the defendants' acts or omissions i.e. if an injury cannot be reasonably connected to the negligent activity.[61] As mentioned above, information asymmetries that users face in the digital economy

[56] Rule 1, Order VII, The Code of Civil Procedure, 1908.
[57] "Complainant" is defined under S. 2(5) of the Consumer Protection Act, 2019 as (i) a consumer (ii) any voluntary consumer association registered under any law for the time being in force (iii) the Central Government or any State Government (iv) the Central Authority under the Act (v) one or more consumers (vi) legal heir or representative of a deceased consumer or (vii) a parent or guardian of a minor.
[58] Supra 35, S. 2(6).
[59] S. 43A, The Information Technology Act, 2000.
[60] Poonam Verma v. Ashwin Patel, AIR 1996 SC 2111.
[61] Bourhill v. Young (1943) AC 92 (1943, House of Lords).

could make it very difficult for users to demonstrate a causal link between a breach or processing activity and harm.[62] The difficulty could be especially higher in case of secondary harms pursuant to data breach, considering that the harms could have emerged from a breach of the users' personal data from another entity.[63] Similarly, complaints made under the CPA for unlawful disclosure of personal data or through the CPC for breach of privacy agreements may only provide redress for the immediate breach of personal data or failing to provide the standard of care defined under contract, but also for secondary harms.

1.2. Users Could Find it Difficult to Show Injury

The second challenge that arises is users being unable to show injury when personal data is breached or processed improperly. Personal data breaches and improper processing of personal data can make users vulnerable to harm and increase risk of harm. However, harm would only be speculative until it actually materializes. Users whose personal data is breached or processed improperly could speculate that they will be harmed, but they cannot be certain about how and when they will be harmed. Users could find it difficult to obtain redress based on such speculations of harm.

In their scholarly work on personal data-related harms "Risk and Anxiety: A Theory of Data Breach Harms," Daniel Solove and Danielle Citron (2017) present a trend of cases on speculation of harm due to data breaches that were adjudicated by courts in the United States of America ("**USA**").[64] These cases cover three overarching arguments from users seeking redress: "(i) data breaches create a risk of future injury, (ii) plaintiffs take preventative measures to reduce risk of injury, and (iii) plaintiffs experience anxiety as a result of data breaches compromising their personal data."[65] The courts seem to have rejected the first argument (risk of future injury) for being too speculative even in cases where personal data was breached by thieves. The courts seem to have rejected redress when they were unable

[62] Supra 11; See Supra 48.
[63] Supra 2; D.J. Solove, *Privacy and Data Security Violations: What's the Harm?*, TeachPrivacy, available at https://www.linkedin.com/pulse/20140625045136-2259773-privacy-and-data-security-violations-what-s-the-harm/, last seen on 30/11/2020.
[64] Supra 48.
[65] Ibid at 9.

to find immediate harm from the breach or when the period when harm could occur was unascertainable, even if the risk of harm increased greatly.[66] The second argument (preventative measures to reduce risk) seems to have been rejected by the courts on the ground that users could use such measures to 'manufacture' injury.[67] The courts seem to have rejected the third argument (anxiety as a result of a data breach) on grounds that anxiety stemmed from the speculation of harm, and not on certainty of impending harm.[68] The argument seems to have been rejected unless plaintiffs were able to demonstrate impending harm and emotional distress.[69] These judgements are useful in understanding the difficulties that users in India could face in demonstrating injury.

Therefore, although users could hold providers liable for personal data breaches under the existing frameworks, users may not be able to establish a cause of action and demonstrate injury to get redress for secondary harms.

2. Challenges for User Protection and Redress Under the Upcoming Personal Data Protection Bill, 2019

The Bill seeks to create a distinct and elaborate framework to regulate personal data processing[70] activities in India and protect users' interests

---

[66] Ibid at 10; Key v. DSW, Inc., 454 F. Supp.2d 684 (2006, United States District Court, S.D. Ohio, Eastern Division); In re Science Applications International Corp (SAIC) Backup Tape Data Theft Litigation, No. MDL 2360, 2014 U.S. Dist. LEXIS 64125 (D.D.C, May 9, 2014). The courts accepted the argument in cases where the harm was "immediate and very real," such as when unauthorized transactions appeared in users' bank accounts (See Remijas v. Neiman Marcus Group (7th Cir. 2015)) or when new bank accounts were attempted to be opened post a data breach (See Krottner v. Starbucks Corp., 628 F.3d 1139 (2010, United States Court of Appeals, Ninth Circuit)).

[67] Supra 48; Polanco v. Omnicell, Inc (2013, United States District Court of New Jersey).

[68] Ibid; Crisafulli v. Ameritas Life Insurance Co., 2015 WL 1969173 (2015, United States District Court of New Jersey); In re Barnes & Noble Pin Pad Litigation, No. 12-cv-8617, 2013 WL 4759588 (2013, United States District Court for the Northern District of Illinois Eastern Division); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (2009, United States District Court, E.D. Missouri, Eastern Division).

[69] Crisafulli v. Ameritas Life Insurance Co., 2015 WL 1969173 (2015, United States District Court of New Jersey); Maglio v. Advocate Health & Hospitals., 49 N.E. 3d 746, 755 (Ill. App. 2015).

[70] This paper relies on the definition of 'Processing' under the draft Personal Data Protection Bill, 2019 that defines 'Processing' under S. 3 (31) as: "*an operation or set of operations performed on personal data, and may include operations such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction*".

from harm *ex ante*.[71] The framework prescribes obligations for data fiduciaries,[72] rights for data principals[73] and powers and functions of the proposed Data Protection Authority (**"DPA"**).[74] However, the Bill predicates twenty-three crucial provisions on the occurrence of 'Harm' as defined in the Bill: It uses harm as a trigger for the enforcement of crucial rights, obligations and regulation.[75] This harms-based approach of the Bill could create practical challenges that significantly weaken its ability to protect users and provide redress.

The problems with the definition of 'Harm' in the Bill have been discussed in S. 3 of this article. The definition is vague, open-ended and very difficult to interpret. In the absence of any guidance in the definition to understand its scope, the task of identifying 'Harm' is left to the subjective interpretation of different stakeholders.[76] This is problematic because what a user interprets as 'Harm' could be interpreted differently by a provider or a regulator.[77] For instance, a user might consider anxiety from personal data breaches as harm, but providers and regulators may be more conservative in their interpretation.[78] This uncertainty could confuse stakeholders about how they should act to mitigate and remedy harm, and compromise the Bill's goal of *ex ante* protection. Users would remain uncertain about whether they have been harmed and whether they can seek redress. Providers and other entities that process personal data would remain uncertain about how to design and conduct data processing activities. Regulators and adjudicators would remain uncertain about when and how

---

[71] Preamble, The Personal Data Protection Bill, 2019 (pending).
[72] 'Data fiduciary' is defined under S. 3(13) of the Bill as "*any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data*."
[73] 'Data principal' is defined under S. 3 (14) of the Bill as "*the natural person to whom the personal data relates*."
[74] Supra 8, S. 49.
[75] *Our Submission to the Joint Committee of Members of the Indian Parliament on the Personal Data Protection Bill*, dated 25 February 2020, p. 19, Dvara Research, available at https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf, last seen on 29/11/2020. Three provision relate to data principals exercising their rights and accessing grievance redress forums. Nine provisions relate to the fulfilment of data protection obligations by data fiduciaries. Eleven provisions relate to the enforcement of the Bill by the Central Government and the DPA.
[76] Supra 44.
[77] Ibid.
[78] Supra 48.

to intervene in data processing activities or provide redress to mitigate and remedy harm.[79]

For example, the provision on 'reporting of personal data breach'[80] is one of the most important user protections safeguards in the Bill. The provision directs data fiduciaries to alert the proposed data protection regulator, the DPA, about personal data breaches so that they may direct necessary actions to mitigate harm from the breach. However, the provision requires data fiduciaries to report personal data breaches only when there is a likelihood of harm. Therefore, when personal data is breached, data fiduciaries can make a subjective assessment of whether the breach can cause harm (as defined in the Bill). Only once it determines that harm could occur does it have to report the breach to the DPA. This risks many sensitive data breaches not being reported to the DPA because data fiduciaries cannot identify or predict harms easily (This is besides the fact that it may be in the interests of data fiduciaries to not report personal data breaches to the DPA).[81] Users would remain vulnerable to secondary harms that could arise when the breached data is processed for *mala fide* purposes.[82]

Similarly, the provision on 'Grievance redress'[83] allows data principals to seek redress when data fiduciaries contravene provisions of the Bill. However, harm or the likelihood of harm are the necessary preconditions for data principals to seek redress. This precondition raises high barriers for seeking redress. It would preclude users from seeking redress when there is (i) a violation of the Bill without corresponding harm or (ii) a harm but without any violation of the Bill.[84] The precondition also levies a disproportionately heavy burden on the users to demonstrate that harm could occur because of the data fiduciary violating a provision in the Bill.[85]

---

[79] Supra 44.
[80] Supra 8, S. 25.
[81] Supra 44.
[82] R.J. Cronk, *Why Privacy-Risk Analysis Must Not be Harm Focused*, IAPP, available at https://iapp.org/news/a/why-privacy-risk-analysis-must-not-be-harm-focused/, last seen on 30/11/2020.
[83] Supra 8, S. 32.
[84] *Our Response to the Draft Personal Data Protection Bill, 2018*, Dvara Research, available at https://www.dvara.com/blog/wp-content/uploads/2018/10/Response-to-draft-Personal-Data-Protection-Bill_DvaraResearch.pdf, last seen on 29/11/2020.
[85] Supra 44.

The precondition assumes that users will have knowledge of all processing activities and their effects and that they will be able to identify and demonstrate harm. However, as mentioned above, information asymmetries that users face could make it impossible for them to do so.[86]

Other key provisions in the Bill that are linked to harm would be impacted by similar challenges. Although harm is an important factor to consider in user protection, it cannot be the yardstick for protecting users against personal data-related harms. Harm can be an outcome that regulation can protect against, but harm should not be the trigger for regulation. Data protection frameworks must be designed to be independent of harm to be effective in protecting users from harm.[87] Defining the rights of users and the responsibilities of providers in a way that imposes an obligation on providers to make reasonable efforts to not cause harm could be a more suitable approach for user protection in data processing activities.[88] Yet, the question about how harm should be defined remains to be answered.

V. DEFINING 'HARM': ENABLING A GRADUAL JURISPRUDENTIAL EVOLUTION OF THE DEFINITION

The article so far has discussed how personal data-related harm is unique. These harms can manifest in many forms, including in visceral and tangible forms, and at any point in time once personal data is breached or processed

---

[86] Supra 11; Also see D.J. Solove& D. Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, GWU Law School Public Law Research Paper No. 2017-2, 1, GWU Law School Public Law Research Paper No. 2017-2, George Washington University Law School, (2017), available at https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2499&context=faculty_publications.

[87] Supra 44; *Our submission to the Joint Committee of Members of the Indian Parliament on the Personal Data Protection Bill*, dated 25 February 2020, p. 19, Dvara Research, available at https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf, last seen on 29/11/2020; R.J. Cronk, *Why Privacy-Risk Analysis Must Not be Harm Focused*, IAPP, available at https://iapp.org/news/a/why-privacy-risk-analysis-must-not-be-harm-focused/, last seen on 30/11/2020.

[88] See Supra 84; *Our Response to the White Paper on a Data Protection Framework for India*, Dvara Research, available at https://www.dvara.com/blog/wp-content/uploads/2018/02/Response-to-White-Paper-Public-Consultation-Dvara-Research.pdf, last seen on 30/11/2020; and *The Data Protection Bill, 2018*, p.3, Dvara Research, available at https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf, last seen on 30/11/2020; Also see D. Solove, *How Should the Law Handle Privacy and Data Security Harms?*, TeachPrivacy, available at https://teachprivacy.com/law-handle-privacy-data-security-harms/, last seen on 24/12/2020.

improperly. Further, the harms can manifest in new and inchoate forms that could emerge with developments in data processing technology and use-cases. These characteristics of harm make it impractical to create a prescriptive definition of 'Harm' (such as that under S. 3(20) of the Bill). The sheer scope of personal data-related harm makes it impossible to posit all the different kinds of outcomes that must be treated as harm without becoming vague. Not defining harm at all on the other hand could be as problematic as having an expansive definition.

Attempts to define harm could take a middle path in which the definition can broadly indicate what harm means without attempting to be too specific. The definition could guide the gradual development of jurisprudence on personal data-related harm on a case-by-case basis.[89] Simultaneously, the developments could guide providers' data practices in order to mitigate the risk of causing harm to users.[90] A potential definition for this purpose could contain a fundamental or conceptual understanding of harm; such as:

> 'Harm' is actual or potential injury or loss to an individual, whether such injury or loss is economic or non-economic, quantifiable or non-quantifiable.[91]

This definition builds upon existing notions of harm that are already being used by regulators to address harm and the risk of harm when it is difficult to identify. For instance, the Federal Deposit Insurance Corporation ("**FDIC**") relies on this definition for guiding its enforcement activities

---

[89] *Our Response to the White Paper on a Data Protection Framework for India*, p.59-60, Dvara Research, available at https://www.dvara.com/blog/wp-content/uploads/2018/02/Response-to-White-Paper-Public-Consultation-Dvara-Research.pdf, last seen on 02/12/20.

[90] Ibid; *Our Submission to the Joint Committee of Members of the Indian Parliament on the Personal Data Protection Bill*, dated 25 February 2020, p. 20, Dvara Research, available at https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf, last seen on 29/11/2020.

[91] S. 2 (m), The Data Protection Bill, 2018, available at https://www.dvara.com/blog/wp-content/uploads/2018/02/Data-Protection-Bill-Draft-Dvara-Research.pdf; FDIC Consumer Compliance Examination Manual- June 2019, p. 2.1., Federal Deposit Insurance Corporation, available at https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/2/ii-2-1.pdf, last seen on 02/12/2020; Supra 87; *Our Submission to the Joint Committee of Members of the Indian Parliament on the Personal Data Protection Bill*, dated 25 February 2020, p. 20, Dvara Research, available at https://www.dvara.com/research/wp-content/uploads/2020/03/Dvara-Research-Final-Submission-Comments-to-the-Joint-Parliamentary-Committee-on-PDP-Bill.pdf, last seen on 29/11/2020.

towards identifying, addressing, preventing and remedying consumer harm from financial institutions.[92]

Admittedly, the definition appears similar to that of 'Harm' in the Bill, but with prominent distinctions. The definition under the Bill attempts to list the different kinds of personal data-related harm. The definition was also open-ended without a defined scope within which outcomes could be treated as harm. The definition proposed above does not attempt to list the various kinds of personal data-related harms. It draws broad contours i.e., all actual or potential injuries, economic and non-economic injuries and quantifiable and non-quantifiable injuries, that firmly define its scope within which outcomes should be treated as harm.

These contours in the definition proposed above would guide courts in examining harm in each case and gradually developing jurisprudence through precedent. The contours would also set broad goalposts that can guide stakeholders in identifying the boundaries of legitimate activity. This could allow the stakeholders to take necessary steps: such as designing processing activities, approaching regulators for redress or taking enforcement action towards mitigating and redressing harm. Such a definition would be useful in addressing the elusive issue of identifying personal data-related harm until there is a better understanding about how the unique challenges posed by personal data-related harm can be addressed.

VI. CONCLUSION

India is making strides towards becoming a digital economy. A host of public entities and private entities are able to provide digital services for users' benefit. More users in India are becoming digitally active for these services in turn and are generating large amounts of personal data in the process. These gains and benefits could be undone if users' privacy and interests are not safeguarded in this new digital ecosystem. The law must

[92] *FDIC Consumer Compliance Examination Manual- June 2019*, p. 2.1-2.3, Federal Deposit Insurance Corporation, available at https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/2/ii-2-1.pdf, last seen on 02/12/2020.

keep pace with technical developments to make the ecosystem safe for users.

Unfortunately, personal data-related harms pose unique challenges to user protection. It is very difficult to discern what kinds of harm can emerge from personal data processing and to predict when they may emerge once personal data is processed. Together, these factors complicate user protection greatly. One of the biggest complications for the law lies in defining personal data-related harms for the purpose of regulation. For instance, in an attempt to define 'Harm' exhaustively as a list of outcomes, the Bill posits a vague and overbroad definition of 'Harm'. As a result, it risks weakening and diluting several regulatory and user protection provisions in its framework.

Currently, there is inadequate understanding about personal data-related harms among stakeholders involved. Until personal data-related harms are understood better, the law could rely on existing notions of harm that are already being used by regulators to address harm and the risk of harm when it is difficult to identify. The jurisprudence on personal data-related harms and the finer nuances could be developed gradually on a case-by-case basis. Such an approach could be more practicable and helpful in user protection. The law is most effective in safeguarding users' interests when it is practicable.

CRIMINAL SANCTIONS, PRODUCT-LIABILITY REGIME AND EMERGING ISSUES OVER AI AND ROBOTICS UNDER THE CONSUMER PROTECTION ACT, 2019

[*]Arjun Chatterjee & [**]Vageesh Sharma

ABSTRACT

The introduction of Consumer Protection Act, 2019 ("Act") has critically affected the liability framework in cases pertaining to consumer disputes. Though monetary compensation has been provided as recourse to a wronged consumer under several existing laws, the new legislation takes a step ahead by imposing criminal sanctions on different stakeholders ranging from manufacturers of a product to its sellers. We will examine the Act in light of the prevalent international standards and it will be argued that the criminal punishment will not serve as a blanket boon to consumers across all the industries.

Another significant contribution of the Act is the 'product-liability' framework. With the advent of consumer capitalism, we are increasingly living in a commodified world. We will look at how product liability laws have developed over the years and has helped balance the skewed power relations between consumers and corporations. As a codified law, we will analyze the remedies available under the product-liability regime vis-à-vis other special laws with the help of judicial precedents.

The advancement of technology in the creation of Artificial Intelligence ("AI") system and robots has led to many challenges in imputing the liability. These new technologies have influenced the patterns of consumption and have created new vulnerabilities for consumers. The paper furthers a discussion on their personal safety and data security. In view of the existing legal vacuum in India, we shall make some suggestions in addressing the concerns.

[*] Arjun Chatterjee, Graduate of 2013-18 batch, WBNUJS, Kolkata.
[**] Vageesh Sharma, Graduate of 2013-18 batch, WBNUJS, Kolkata, and a practicing Advocate in the State of Rajasthan.

I. INTRODUCTION

The Consumer Protection Act, 2019 ("**Act**") considerably expanded the focus of consumer law in India by the introduction of new aspects: the imposition of criminal liabilities in consumer actions and product liability for defective products. The Act also comes at the cusp of an anticipated technological revolution in Artificial Intelligence ("**AI**") and Robotics. Our primary focus in this work therefore is to critically evaluate the new introductions in law while anticipating future challenges that may arise. Our article is divided into three parts. In Part I, we examine the consumer protection laws in China and the United States of America ("**USA**") to comprehend the strict applicability of criminal liability and high compensation, respectively in both countries. Subsequently, we proceed to argue that the introduction of criminal liability remains ineffective for ensuring consumer protection except in cases of misleading advertisements, where the intentional wrongdoing of the different stakeholders ought to attract criminal sanctions. In Part II, the product liability regime, as introduced by the new legislation, is thoroughly discussed. Tracing its origins, the paper highlights that the modern law provides considerable scope for imposing liability on third party intermediaries in the supply chain. In Part III, the imposition of liability on artificial intelligence systems is explored within the present legislation and the future challenges in attributing different forms of liability on AI systems are presented.

PART- I

II. CONSUMER PROTECTION LAWS IN INDIA AND FOREIGN COUNTRIES: AN OUTLOOK

The term 'consumer' has been widely drafted under Indian law[1] and interpreted by the courts in various domains of life. A consumer can mean

[1] S. 2 (1) (d), The Consumer Protection Act, 1986 (stands repealed). It defines 'consumer' as a person who:
(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system

the intended beneficiary of goods or services with the due consent of the original purchaser in a material transaction[2] or a landowner who entrusted his house construction to a contractor.[3] Even a car purchaser, who intends to use it as a taxi for self-employment, is held to be a consumer.[4] The omnipresence of consumers led the government and senior economists[5] to advise strong policy measures and prioritize their protection in the market.[6] In pursuance of the objectives enshrined in the National Action Plan, the government formed working groups to identify major consumer interests

of deferred payment when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or
(ii)[hires or avails of] any services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other than the person who [hires or avails of] the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person [but does not include a person who avails of such services for any commercial purpose].
See Kishore Lal v. Chairman, Employees' State Insurance Corpn., (2007) 4 SCC 579- The Supreme Court of India held:
"*The definition of "consumer" in the CP Act is apparently wide enough and encompasses within its fold not only the goods but also the services, bought or hired, for consideration. Such consideration may be paid or promised or partly paid or partly promised under any system of deferred payment and includes any beneficiary of such person other than the person who hires the service for consideration. The Act being a beneficial legislation, aims to protect the interests of a consumer as understood in the business parlance. The important characteristics of goods and services under the Act are that they are supplied at a price to cover the costs and generate profit or income for the seller of goods or provider of services. The comprehensive definition aims at covering every man who pays money as the price or cost of goods and services. However, by virtue of the definition, the person who obtains goods for resale or for any commercial purpose is excluded, but the services hired for consideration even for commercial purposes are not excluded. The term "service" unambiguously indicates in the definition that the definition is not restrictive and includes within its ambit such services as well which are specified therein. However, a service hired or availed, which does not cost anything or can be said free of charge, or under a contract of personal service, is not included within the meaning of "service" for the purposes of the CP Act.*"
[2] Lucknow Development Authority v. M.K. Gupta, (1994) 1 SCC 243.
[3] Faqir Chand Gulati v. Uppal Agencies Pvt. Ltd., (2008) 10 SCC 345; Bunga Daniel Babu v. Sri Vasudeva Constructions, (2016) 8 SCC 429; Sujit Kumar Banerjee v. Rameshwaran, (2008) 10 SCC 366.
[4] Hindustan Motors Ltd. v. N.P. Tamankar, (1996) CPJ 313 (NC).
[5] Dr. H. A. C. Prasad & R. Sathish, *Policy for India's Services Sector*, Working Paper No.1/2010-DEA, 22, Department of Economic Affairs, Government of India (2010) available at https://dea.gov.in/sites/default/files/policy%20Paper%20on%20Services%20Sector.pdf, last seen on 02/11/2020.
[6] Ministry of Consumer Affairs, Food and Public Distribution, Government of India, *Report of the Working Group on Consumer Protection Twelfth Plan (2012-17) Volume – I,* available at https://niti.gov.in/planningcommission.gov.in/docs/aboutus/committee/wrkgrp12/pp/wg_cp1.pdf, last seen on 02/11/2020.
(The subject of Consumer Protection was included as the one of the subjects in the priority areas of Niti Aayog, erstwhile Planning Commission's 12th Plan. As a consequence, a working group was formulated to suggest policies and strategies for a better consumer protection regime).

in 6 crucial areas across the country[7] and proposed to utilize INR 200 crores for effectively informing the consumers about their rights and entitlements.[8] Furthermore, the creation of informal modes of dispute resolution led to the redressal of nearly 95 percent of the consumer grievances in the financial year 2018-19[9], which raises the discussion on the nature of liabilities and consequent consumer satisfaction enlisted under the traditional legal regime of consumer protection laws in India.

Similar to most common law countries, the dispensation of justice under Indian consumer law is governed by the statutory quasi-judicial forums, which have powers similar to those vested in a court of law.[10] After duly following the established procedure by appreciating evidence[11] and hearing both the parties, if in the opinion of the forum(s), the averments in a 'complaint'[12] stand proven, then the opposite party may be liable for restoring the *status quo* of the consumer.[13] The failure of either of the

---

[7] *National Action Plan For Consumer Awareness*, Consumer Affairs, available at https://consumeraffairs.nic.in/organisation-and-units/division/consumer-welfare-fund/national-action-plan-for-consumer-awareness, last seen on 02/11/2020. (The six marked areas were food safety, misleading advertisements, drugs pharmaceuticals and medical devices/equipment, consumer health & safety concerning tobacco products, counterfeit/fake/spurious/contraband products, and proposals to amend the existing consumer laws incorporating the aspects of product liability law, unfair terms of contract act, builders' licensing boards act and whistle blowers act).

[8] Ibid.

[9] Ministry of Consumer Affairs, Food and Public Distribution, Government of India, *Annual Report 2018-19,* available at https://consumerhelpline.gov.in/assets/annual-reports/Annual_Report_2018-19.pdf, last seen on 02/11/2020. (The government set up a National Consumer Helpline vide an Integrated Grievance Redressal Mechanism (INGRAM) which provides a platform for all the concerned stakeholders to resolve the grievances. Notably the maximum number of complaints/grievances were registered in the e-commerce sector and a maximum of 99% grievances were resolved through this process in the financial year 2017-18).

[10] Laxmi Engineering Works v. P.S.G. Industrial Institute, (1995) 3 SCC 583. The Supreme Court held:

"*A review of the provisions of the Act discloses that the quasi-judicial bodies/authorities/agencies created by the Act known as District Forums, State Commissions and the National Commission are not courts though invested with some of the powers of a civil court. They are quasi-judicial tribunals brought into existence to render inexpensive and speedy remedies to consumers. It is equally clear that these forums/commissions were not supposed to supplant but supplement the existing judicial system. The idea was to provide an additional forum providing inexpensive and speedy resolution of disputes arising between consumers and suppliers of goods and services.*"

For the purposes of this part of the essay, the three forums namely, the National Commission, State Commission and the District Forum are collectively referred to as forums.

[11] S. 13, The Consumer Protection Act, 1986. (stands repealed)

[12] Ibid, S. 2 (1) (c).

[13] Ibid, S. 14 (The opposite party may be asked to *inter alia* remove the identified defect in the product, or replace the goods with new ones, or return the price(s)/charges paid by the consumer, or pay compensation for any the loss suffered by the consumer or the opposite party may be liable for punitive damages).

contesting parties to abide by an order passed by any of the forums attracts criminal liability.[14] While the erstwhile Indian consumer statute provided for criminal punishment only in cases of non-adherence to the order of forums, other countries, for instance, China and the USA, enlist such penalties if any harm is proved to a consumer, thereby following a stricter punishment regime. The paper highlights the consumer laws therein and argues that even the strictest of punishments lack credibility and support from the consumer industry. These States are selected for this paper to show that even the most rigid and inflexible consumer laws from the common and civil law countries remain of very little help when it comes to ensuring justice to the consumers.

Although the Indian jurisdiction permitted criminal sanctions in specific circumstances, the data revealing complaints' disposal indicates utmost satisfaction. As per the latest available statistics by the government, slightly over 80 percent of the complaints filed in these forums at the state and national level have been disposed of, whereas the figure is over ninety percent at the district level.[15] However, do the rates of disposal reflect squarely on a consumer's desired needs? As per a research conducted in 2018, a majority of the respondents expressed their contentment at the judgments rendered by the forums[16] but, interestingly, more than half of the dissatisfied respondents reasoned delay and insufficient compensation as contributing elements to their disapproval of the decisions.[17] Previous studies also suggest that the number of consumer complaints across the three forums has uniformly increased and, despite the disposal of a substantial number of complaints, there is considerable delay in the process.[18]

---

[14] Ibid, S. 27.
[15] Supra 9.
[16] Marinal Gupta & Sarang Narula, *Complainant Satisfaction with Reference to Consumer Dispute Redressal Forum*, 3 International Journal of Social Science & Economic Research 2012, 2021(2012), available at http://ijsser.org/2018files/ijsser_03__139.pdf, last seen on 03/11/2020.
[17] Ibid, at 2025.
[18] Elwin Paul Konattu & V.K. Sudhakaran, *A Critical Evaluation on the Performance of Consumer Disputes Redressal Commission in India*, 20 IOSR Journal of Business and Management 47, 50-51 (2018), available at http://www.iosrjournals.org/iosr-jbm/papers/Vol20-issue9/Version-4/F2009044752.pdf, last seen on 03/11/2020.

The paper selects a few relevant legislations to inform the reader about the nature of liabilities and grievance redressal mechanisms stipulated therein. While these legislations are specifically consumer-oriented and provide for criminal punishments and monetary compensation in case of a violation, the domestic scenario reveals that both the aforesaid remedies do not suffice and therefore, there remains a requirement for the state to act preventively by means of stricter pre-harm actions. Thus, even if the forums adjudicate consumer disputes by awarding suitable compensation as damages to cure the harm, the delay caused in the process remains a major disincentive for the consumer to approach such forums. Alternatively, criminal punishments imposed in civil countries such as China seemingly appear to be an efficacious remedy, but only suitable prevention mechanisms by the state can fully aid in ensuring a consumer-friendly environment.

1. China

The most relevant example of a civil law country that provides for seemingly stringent regulations in cases of consumer harm remains that of China. In 2008, the notorious sentencing of Sanlu officials to life imprisonment, for being associated with the illicit contamination of the drinking milk, enlarged the state's role in successfully prosecuting those involved in a deliberate attempt to harm its citizens[19], in what is considered as one of the most hazardous incidents relating to consumers' health across the globe. However, this incident raised the pertinent question of the primary liability of the state itself.

[19] Yungsuk Karen Yoo, *Tainted milk: What Kind of Justice for Victims' Families in China*, 33(2) Hastings Int'l & Comp. L. Rev. 555,557 (2010), available at https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1745&context=hastings_international_comparative_law_review, last seen on 31/10/2020. Though a few young infants were directly affected by the contaminated milk, the strenuous state action in ensuring imprisonment for the responsible officers reflected the plight of the affected parents as concerned citizens; See Exim Brickell LLC v. PDVSA Services INC., 516 Fed. Appx. 742 (2013, Court of Appeals for the Eleventh Circuit). Although the appeals' court upheld the decision of the district court in awarding partial damages to the purchaser Bariven S.A., a Venezuelan state-owned company, as per the agreed contractual terms in a civil dispute which involved an inter-country milk trade, the judgment observed that after the discovery of melamine contamination in the milk, the Chinese government barged in the industry and prohibited further sale of the milk.

Even though the present Chinese law penalizes the violation of the hygiene standards with a heavy compensation[20] and exposes the offenders to criminal prosecution in cases of harm to human health[21], its critics remain skeptical of its implementation in punishing every stakeholder involved in the process.[22] They argue that since the state was the most crucial stakeholder in ensuring safety to its citizens, it was required to act preventively and maintain the consumers' confidence in the market.[23] To its contrary, the news reports suggest that the aggrieved parents of the deceased and infected infants demanded strict legal action against the state officials for having left uncontrolled the contaminated element used in the milk, and censured its offer of a meagre compensation.[24] Therefore, even the strictest liability regime prevalent in the country could not prove satisfactory to the aggrieved consumers.

2. United States of America

[20] Article 39, The Food Hygiene Law of the People's Republic of China 1982, (China).
[21] Article 41, The Food Hygiene Law of the People's Republic of China 1982, (China).
[22] Shumein Chen, *Sham or Shame: Rethinking the China's Milk Powder Scandal from a Legal Perspective*, 12 Journal of Risk Research 725,734 (2009), available at https://www.tandfonline.com/doi/pdf/10.1080/13669870902927251?needAccess=true, last seen on 28/10/2020; See Frederic Keck, *The Contaminated Milk Affair,* 2009/1 China Perspectives 88, 88 (01/04/2009), available at https://journals.openedition.org/chinaperspectives/4780, last seen on 30/10/2020.
[23] Zhe Chen, *The Melamine Milk Scandal and Its Implication for Food Safety Policy in China* 37 (2015) (Published Thesis, Oregon State University) available at https://ir.library.oregonstate.edu/concern/graduate_projects/2r36v0290, last seen on 30/10/2020. The thesis argued that since the contaminated element, namely Melamine, was not regulated by the state and could be accessed by anyone in the market, its potential to be misused increased significantly. As a result, the producers at Sanlu, misused the element in causing death of six infants and severely causing bodily injuries to over three lakh children. Due to the widespread damage, the consumers' faith in the dairy producers and retailers faced a downturn and the government was subjected to heavy criticisms by the consumer industry. For a detailed explanation of the state's significant omissions, See Yanjie Li, *The Aftermath of the Milk Scandal of 2008- The Challenges of Chinese Systemic Governance and Food Safety Regulation* 32 (2015) (Published Thesis, University of Warwick, School of Law) available at http://wrap.warwick.ac.uk/98045/1/WRAP_Theses_Li_2015.pdf, last seen on 29/10/2020.
[24] The Associated Press, *Parents in China's Milk Scandal Criticize Payout,* NBC News (31/12/2008), available at https://www.nbcnews.com/health/health-news/parents-chinas-milk-scandal-criticize-payout-flna1C9444094, last seen on 30/10/2020.

Although consumer rights are regulated under different State and Federal laws in the USA[25], in some cases, the latter pre-empts the former.[26] The central objective across different state laws, for instance, in California, is to highlight the liability of the manufacturers who provide implied warranties to the consumers.[27] In this jurisdiction, as opposed to the civil law of China, the consumers are ensured with a huge financial penalty in case of a breach of their rights[28]. Yet, the desired consequence of the deterrence effect upon the manufacturers remains far from reality.[29] While the state laws focus on

[25] Jacques Delisle & Elizabeth Trujillo, *Consumer Protection in Transnational Contexts,* 58 AM. J. COMP. L. 135, 136 (2010), available at https://scholarship.law.tamu.edu/cgi/viewcontent.cgi?article=1802&context=facscholar, last seen on 31/10/2020.

[26] Trans World Airlines v. Mattox., 712 E Supp. 99 (1989, U.S. District Court for the Western District of Texas)- The central issue in this litigation was whether the allegedly deceptive advertisements issued by the plaintiff can be regulated by issuance of an injunction order following the states' statutes above the Airline Deregulation Act of 1978 which was the prevalent federal law. The district court ruled in favour of the plaintiff by holding that the injunction order cannot be issued by the states under the purview of regulating the advertisements and the view was upheld by the Supreme Court in Morales v. Trans World Airlines, 504 U.S. 374 (1992, U.S. Supreme Court); See Colin Provost, *The Politics of Consumer Protection: Explaining State Attorney General Participation in Multi-State Lawsuits*, 59 Political Research Quarterly 609, 610 (2006), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579833, last seen on 31/10/2020.

[27] Eileen K. Jenkins, *Consumer Protection: The Effect of the Song-Beverly Consumer Warranty Act*, 4 Pac. L. J. 183, 196 (1973), available at https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1510&context=mlr, last seen on 01/11/2020; See Greenman v. Yuba Power Products Inc., 59 Cal.2d 57 (1963, Supreme Court of California)- The Supreme Court while awarding the damages to the plaintiff held, that a manufacturer need not give an express warranty of a product. It is sufficient for the plaintiff to show that he suffered damage out of a defective product which was placed on the market by the manufacturer knowing the purpose for which it was to be used. The Court held the manufacturer liable on the principle of strict liability.

[28] The Song-Beverely Consumer Warranty Act (1970) S. 1793.2(d) (United States).

[29] Shauhin A. Talesh, *The Privatization of Public Legal Rights: How Manufacturers Construct the Meaning of Consumer Law*, 43 Law & Society Review 527, 554 (2009), available at https://www.jstor.org/stable/40538715?seq=1, last seen on 01/11/2020; See The Song-Beverely Consumer Warranty Act (1970) S. 1794.2 (United States)- The primary reason of the failure to achieve the desired legislative intent behind this law was the evacuative route provided within it. The manufacturers used this provision to argue that they are not liable to the consumers as they adopted the third-party resolution process and furthermore, the buyer did not issue a notice as provided in the provisions. Even in cases where the buyer supplied the manufacturer with a notice, the latter's compliance of paragraph (2) of subdivision (d) of Section 1793.2 will relieve him from its civil penalty towards the buyer. Paragraph (2) of subdivision (d) of Section 1793.2 is reiterated herein: "*If the manufacturer or its representative in this state is unable to service or repair a new motor vehicle, as that term is defined in paragraph (2) of subdivision (e) of Section 1793.22, to conform to the applicable express warranties after a reasonable number of attempts, the manufacturer shall either promptly replace the new motor vehicle in accordance with subparagraph (A) or promptly make restitution to the buyer in accordance with subparagraph (B). However, the buyer shall be free to elect restitution in lieu of replacement, and in no event shall the buyer be required by the manufacturer to accept a replacement vehicle.*" Thus, the maximum relief that a buyer could receive is that of restitution of his defective products from the manufacturer.

high compensation, some of the federal laws focus on prohibiting the "unfair trade practices" causing harm to the consumers.[30] Even though the anti-competitive measures are duly regulated, heavy compensations fail in ensuring consumer satisfaction in the country.[31]

III. INCORPORATION OF CRIMINAL LIABILITY UNDER THE CONSUMER PROTECTION ACT, 2019- A STEP AHEAD?

With a significant increase in foreign investment in the consumer goods industry of the Indian economy and owing to increasing demand, the production of goods has increased proportionately,[32] leading to a rise in the possibility of manufacturing errors and irregularities. Since consumers are the ultimate desired recipients of the goods and services[33] and their satisfaction is of paramount importance in India's economic growth,[34] the central consumer protection law has been revamped with provisions relating to criminal prosecution[35] and prompt deliverance of justice, with the fundamental assumption that the institutional mechanism will adequately serve the consumers.

The Indian Parliament passed the Consumer Protection Act, 2019 on 6th August, 2019 with the 'swift executive remedy'[36] of criminal punishment. Besides the provisions for mediation[37] and a central authority to regulate consumer protection,[38] the Act provides for prosecution for both an act

---

[30] 15 U.S.C. S. 52 (United States).
[31] Ibid, at 29.
[32] *Indian Consumer Durables Industry Analysis*, Indian Brand Equity Foundation, available at https://www.ibef.org/industry/consumer-durables-presentation, last seen on 03/11/2020.
[33] Rameshchandra Kachardas Porwa v. State of Maharashtra, (1981) 2 SCC 722. (The Supreme Court held: "*The marketing of agricultural produce is not con-fined to the first transaction of sale by the producer to the trader but must necessarily include all subsequent transactions in the course of the movement of the commodity into the ultimate hands of the consumer, so long, of course, as the commodity retains its original character as agricultural produce.*").
[34] Sanjeev Saxena & Mayank Jindal, *Customer Satisfaction on Banking Services in Indian Growing Economy Nainital District,* 9 International Journal of Engineering and Management Research 74, 74 (2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3479582, last seen on 03/11/2020.
[35] The pre-requisites of criminal liability along with its socio-legal implications in the consumer protection law are discussed in the next section.
[36] *Landmark Consumer Protection Bill, 2019 gets Parliamentary approval*, Press Information Bureau, available at https://pib.gov.in/PressReleseDetailm.aspx?PRID=1581384, last seen on 03/11/2020.
[37] S. 37, The Consumer Protection Act, 2019.
[38] Ibid, S. 10.

and an omission that leads to different forms of injuries.[39] The Parliamentary Standing Committee on Food, Consumer Affairs and Public Distribution observed that the existing legal framework does not offer strong protection to the consumers and has remained unsuccessful in generating sufficient deterrence for the wrongdoers.[40]

The United Nations (**"UN"**) Guidelines[41] stipulate that the maximum penalty, in cases of defective/hazardous products, is their repair and/or replacement with its equivalent, or adequate compensation, if the former is not feasible within a reasonable time. While the guidelines are mere recommendations and non-binding on the nation-states,[42] it is argued that the criminal sanctions will serve no purpose in disputes where no harm is caused to the consumers.[43] Although there are no uniform standards for adopting the nature of liabilities at the global level, research in the field of consumer protection suggests that increased financial penalty will be the most appropriate relief for addressing a consumer's grievance in the Indian jurisdiction and the criminal prosecutions should be saved for the gravest of crimes and repeat offenders.[44]

---

[39] Ibid, S. 88.

[40] Standing Committee on Food, Consumer Affairs and Public Distribution, Lok Sabha, *The Consumer Protection Bill, 2015*, 2016. (The Committee noted that eminent personalities, as brand ambassadors, endorse products which is appealing to the consumers. As a result, several unrealistic claims are made by the promoters of a product which, seemingly impossible, are relied upon by the consumers in their daily lives. Thus, the Committee recommended that there should be a strict deterrent action to regulate the misleading advertisements as well as fixation of liability on the endorsers/celebrities). The term 'wrongdoers' is further discussed in the forthcoming section; See Ministry of Health and Family Welfare, Government of India, *Report of the Expert Committee on a Comprehensive Examination of Drug Regulatory Issues including the problem of Spurious Drugs*, available at https://pharmaceuticals.gov.in/sites/default/files/MashelkarCommitteeReport.pdf, last seen on 04/11/2020. (The Expert Committee observed that there should be severe punitive action on the criminal acts of the manufacturers and distributors of drugs, which can potentially lead to mortality or a threat to the life of innocent consumers).

[41] U.N. General Assembly, *United Nations Guidelines for Consumer Protection*, Res. 39/248, 12, available at https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf, last seen on 04/11/2020.

[42] David Harland, *Implementing the Principles of the United Nations Guidelines for Consumer Protection*, 33 Journal of the Indian Law Institute 189,196 (1991), available at http://14.139.60.114:8080/jspui/bitstream/123456789/17362/1/005_Implementing%20the%20Principles%20of%20the%20United%20Nations%20Guidelines%20for%20Consumer%20Protection%20%28189-245%29.pdf, last seen on 04/11/2020.

[43] See section 'C'.

[44] *Best Practices for Consumer Policy: Report on the Effectiveness of Enforcement Regimes*, The University of Manchester, available at https://www.research.manchester.ac.uk/portal/en/publications/best-practices-for-

1. Issue of Jurisdiction: A Precursor in Establishing Liability

There has been a noticeable shift in the consumer markets with foreign brands acquiring a substantial portion in the country's domestic market.[45] Furthermore, the local consumers appreciate the products manufactured in other countries,[46] which raises the pertinent issue of jurisdiction in a case that involves undesirable goods or services received by a particular consumer in his jurisdiction from a specified country. These transactions often occur through the internet network, wherein the consumers are tempted by products in a foreign territory, leading to transnational business.[47] In this regard, the e-commerce rules recently enacted by the Indian Parliament remain fairly comprehensive. The said rules are applicable to nearly every entity that deals in e-commerce[48] and cover all goods and services transacted through such means.[49]

The basic tenets of international law provide that the laws formed in a nation-state apply within its geographical boundaries.[50] Generally, a similar principle applies to the criminal law of a country.[51] But since the Indian criminal law applies extraterritorially, it implies that, if any person outside Indian jurisdiction commits a punishable offence under any Indian law,[52] he can be tried within the realms of the Indian jurisdiction.

---

consumer-policy-report-on-the-effectiveness-of-enforcement-regimes(fe0b58d3-d8ac-452f-b118-8e9eeaede8d5).html, last seen on 04/11/2020.

[45] S.L. Rao, *India's Rapidly Changing Consumer Markets*, 35(40) Economic & Political Weekly 3570, 3571 (2000) available at https://www.jstor.org/stable/pdf/4409803.pdf?refreqid=excelsior%3A6541163c68fab77f5c1bd2e3534de577, last seen on 04/11/2020.

[46] Robert D. Schooler & Don H. Sunoo, *Consumer Perceptions of International Products: Regional vs. National Labelling*, 49(4) WILEY 886, 887 (1969) available at https://www.jstor.org/stable/pdf/42859967.pdf?refreqid=excelsior%3A2f80a22fa3245ab499362076554fabec, last seen on 04/11/2020.

[47] Lee A Bygrave & Dan Svantesson, *Jurisdictional Issues and Consumer Protection in Cyberspace: The View from Down Under,* 12 Cyber L. Res. (2001) available at http://www.austlii.edu.au/au/other/CyberLRes/2001/12/, last seen on 03/11/2020.

[48] Rule 3(b), Consumer Protection (E-Commerce) Rules, 2020.

[49] Ibid, Rule 2(a).

[50] John Goldring, *Globalization and Consumer Protection Laws*, 8 Macquarie L.J. 79, 83 (2008) available at http://www.austlii.edu.au/au/journals/MqLawJl/2008/6.pdf, last seen on 04/11/2020.

[51] *Consumer Protection, the Nation-State, Law, Globalization, and Democracy*, Wiley Online Library, available at https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.1996.tb00057.x, last seen on 04/11/2020.

[52] S. 3, The Indian Penal Code, 1860 (The Indian Penal Code permits the trial of any person who is liable under Indian law by committing an offence outside India); See Rule

2. Who is Liable?

Before the enactment of the new consumer protection law, the Indian courts acknowledged the prevalent rule of trade practice through the interpretation of similar consumer protection laws.[53] The Courts remarked on the difference in bargaining power between the consumers and the traders, observing that the dominant capacity of the traders is often to the detriment of the consumers.[54] Moreover, the use of anti-competitive practices by several dominant market holders to manipulate consumer choices was also analyzed in detail,[55] which raises the question of imposing liability on the concerned stakeholders.

---

2 (2), Consumer Protection (E-Commerce) Rules, 2020 (The rule is relevant in the context of e-commerce transactions. Although the term is not specifically defined, it broadly covers the online medium which is used for many business activities including sale transactions. The rule covers any entity which is dealing in e-commerce transactions and does not have an establishment in India).

[53] Lakhanpal National Limited v. M.R.T.P. Commission, (1989) 3 SCC 251. (The Supreme Court interpreted S. 36A of the Monopolies and Restrictive Trade Practices Act, 1969 (now repealed), which defined 'unfair trade practices'. The court opined "*When a problem arises as to whether a particular act can be condemned as an unfair trade practice or not, the key to the solution would be to examine whether it contains a false statement and is misleading and further what is the effect of such a representation made by the manufacturer on the common man? Does it lead a reasonable person in the position of a buyer to a wrong conclusion? The issue cannot be resolved by merely examining whether the representation is correct or incorrect in the literal sense. A representation containing a statement apparently correct in the technical sense may have the effect of misleading the buyer by using tricky language. Similarly, a statement, which may be inaccurate in the technical literal sense car, convey the truth and sometimes more effectively than a literally correct statement.*"

[54] Philips Medical Systems (Cleveland) v. Indian MRI Diagnostic and Research Limited and Another, (2008) 10 SCC 227. Markandey Katju J. held "*It is a settled principle of interpretation that when an amendment is made to an Act, or when a new enactment is made, Heydon's mischief rule is often utilized in interpreting the same. Applying this principle, we are of the opinion that Section 36A was inserted in the MRTP Act because there was no provision therein for protection of consumers against false or misleading advertisement or other similar unfair trade practices. It is well-known that in trade suppliers often have a dominant bargaining position, and the bargaining power in the market is often weighed against the consumer. In this situation, it was realized by Parliament in its wisdom when it inserted Section 36A that the public must be prevented from being made victims of false representations about the products sold, even though it may have no adverse effect on competition*."
See Excel Crop Care Limited v. Competition Commission of India, (2017) 8 SCC 47, C. Venkatachalam v. Ajitkumar C. Shah and Ors., (2011) 12 SCC 497.

[55] Telefonaktiebolaget LM Ericsson (PUBL) v. Competition Commission of India, 2016 CompLR 497 (Delhi); In re: Matrimony.com Limited v. Google LLC, Case No. 07 of 2012, (Competition Commission of India, 08/02/2018). Although the Director General who conducted the investigation, found the dominant player, Google in this case, in abuse of its dominant position, by denying the market access to its rival competitors, thereby seriously affecting the consumer choices, the Commission overruled these findings owing to a sheer lack of evidence of any loss or negative influence caused by the firm. It held that a mere position of dominance is not a concern, but the Commission should intervene when the players adopt practices which hamper new innovation or reduce consumer welfare.

The broad definition of 'product seller' under the Act excludes a person who is not a retailer.[56] By deduction, a shop retailer will be covered under the definition. Assuming that there is no express warranty by a retailer, his liability may accrue if the manufacturer cannot be served or is exempt from Indian law,[57] barring the exceptions.[58] In a given case, the retailer may be exempted for acting in good faith.[59] In a proceeding for product liability, a manufacturer can be sentenced to imprisonment for a given period depending upon the nature of the harm suffered by the consumer, even if he proves the absence of negligence or fraudulence in making an express warranty related to a product.[60] This raises a pertinent question: whether the pre-requisites of criminal liability are diluted by the application of different provisions of the Act? The answer can be traced in the next section.

3. Criminal Liability: An Ineffective Tool for Consumer Protection

As highlighted previously, the erstwhile consumer law addressed the consumer grievances by entitling him/her with either a replaced good or suitable compensation, or any other relief as provided therein by an order of the quasi-judicial forums.[61] The Act, in addition to attending to the consumer grievances, enables the consumer to pursue compensation claims for product liability and also provides for criminal litigation against the stakeholders with a corrupt mind.[62]

---

[56] S. 2 (37) (c), The Consumer Protection Act, 2019.
[57] Ibid, S. 86 (d); See Ibid, 2 (20).
[58] Ibid, S. 87.
[59] Ibid, S. 98.
[60] Ibid, S. 84 (2).
[61] Supra 15.
[62] Supra 43; See Mathias Schuz, *Virtue Ethics, Corporate Identity and Success*, 105,106 in *Intrinsic CSR and Competition Doing Well amongst European SMEs* (Walter Wehrmeyer, Mara Del Baldo & Stephanie Looser, 1st ed., 2020). (This article discusses the infamous 'dieselgate scandal' wherein the top executives of the German company Volkswagen, admitted to the U.S. authorities that the company installed 'defeat devices' in cars, which became active while a vehicle is subject to testing and activated equipments, which reduced the emissions of Nitrogen Oxides. Whereas in the regular course of driving the emissions were large in numbers. Apart from achieving its multibillion objectives of dominating the U.S. market through adopting illegal means, the vehicle manufacturer "duped" the consumers by breaching their faith and confidence trusting the brand).

Common prudence suggests that there are multiple reasons to attribute liability on manufacturers, sellers, retailers, and distributors amongst others, as provided under the Act. Primarily, a person aggrieved from suffering an unmediated consequence by the use of a product manufactured by a particular entity in the market, would seek a recourse against that particular entity based on the reason of trust.[63] Secondly, these entities are well-off in the market to securitize their own products.[64] In other words, their market stability accrues from the financial independence which they can utilize to prevent any mishap with a prepared product. Their liability is often vested in civil law, though some jurisdictions have taken a leap ahead in imposing criminal sanctions. However, it's important to analyze the impact of criminal law in society.

As opposed to other laws, the central objective of criminal law as has been aptly described by Joshua Kleinfeld, Professor at Northwestern Pritzker School of Law, is to withhold a community's normative social order.[65] In other words, with the operation of criminal law, a society maintains the ethical standards of living which form the basis of a common order. This inherent social discipline is maintained by the deterrence of a crime's natural consequence, punishment.[66]

Now, let us look at the procedures for initiating criminal actions under different consumer-oriented laws and the interplay between the imposition of criminal punishments and consumer protection. In light of the Covid-19 pandemic, several experts advised people to adopt caution and strictly

[63] Although there arise civil breaches of contract between the consumer-retailers and the consumer-manufacturers above the principle of privity of contract for which a consumer can claim compensation under civil law, this paper's scope covers only the criminal liability.

[64] Fleming James, *General Products-Should Manufacturers be Liable without Negligence*, 24 Tenn. L. Rev. 923, 925 (1997) available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4176&context=fss_papers, last seen on 08/11/2020.

[65] Joshua Kleinfeld, *Reconstructivism: The Place of Criminal law in Ethical Life*, 129 Harv. L. Rev. 1485, 1489 (2016) available at https://harvardlawreview.org/wp-content/uploads/2016/04/1485-1565-Online.pdf, last seen on 05/11/2020.

[66] S. W. Dyde, *Hegel's Conception of Crime and Punishment*, 7 The Philosophical Review 62, 64 (1898) available at https://www.jstor.org/stable/pdf/2175548.pdf, last seen on 05/11/2020.

avoid the use of fake drugs.[67] The reasoning behind the advice was simple: to prevent any adverse effects on their health. The law applicable to drugs in India imposes fines and a punishment stipulating different years of imprisonment on importers, manufacturers, sellers, and distributors of drugs, which are not in accordance with the other provisions of the Act.[68] The criteria for framing charges is the likelihood of a person's death or harm as stipulated in the corresponding provision.[69] Though, the law was drafted during colonial times and subsequently subjected to multiple amendments by the Indian Parliament, the provision for a special court was inserted in the year 2009.[70] This indicates that the lawmakers designed a separate forum for prosecution of the alleged offenders to ensure faster conduct of the trial in public interest.

Similarly, to ensure food safety and avoid any degradation in the food products, provisions related to imprisonment were incorporated in a separate legislation.[71] The punishment was based on the harm caused by the degradation ranging from no injury to death of a person,[72] similar to the protection accorded by the present consumer protection law. But the initiation of the procedure has been clearly defined. Under the food safety law, a food safety officer may collect a sample of the product, which in his opinion is required for any proceedings under the law, and submit it to the food analyst,[73] who then prepares a report and on finding irregularities (if any) in the sample, sends the report to the designated officer.[74] In cases where the sample is found to be in contravention of the standards and is punishable with imprisonment,[75] the designated officer shall recommend prosecution to the Commissioner, who initiates the proceedings against the

[67] *Beware of Fake Anti-COVID Drug Ads: Experts*, National Herald (04/08/2020), available at https://www.nationalheraldindia.com/india/beware-of-fake-anti-covid-drug-ads-experts, last seen on 05/11/2020.
[68] Ss. 13 & 27, The Drugs and Cosmetics Act, 1940.
[69] S. 320, The Indian Penal Code, 1860.
[70] Supra 68, S. 36AB.
[71] S. 59, Food Safety and Standards Act, 2006.
[72] Ibid.
[73] Ibid, S. 38 (1) (c).
[74] Ibid, S. 40 (2).
[75] Ibid, S. 42 (3).

alleged defaulters in a court of law through the designated officer and the food safety officer.[76]

Notably, in the aforementioned examples, either an inspector or a food safety officer may highlight the irregularities in the products through an inspection that could ultimately lead to the punishment of the responsible persons, but the Act does not clarify the procedure for initiating criminal prosecution. Although it can be inferred that prosecution can be initiated through the District Commission, based either on a complaint regarding a defective good,[77] or a derogation of safety standards in place,[78] this aspect needs clarification from government sources, which is presently unavailable to the authors. Furthermore, the Act is a mere reiteration and compilation of the existing laws regarding consumable goods.[79] Even though the provisions are to act in addition to the existing laws,[80] in our view, it adds no substantial provisions including the provisions for prosecution.

Reports from other common law jurisdictions suggest that, while government policies should prioritize consumer welfare rather than ensuring punishment to the traders, a huge compensation can deter the affluent manufacturing corporations.[81] A similar stance has recently been adopted by the Indian legislature. For example, in the automobile industry, the failure to adhere to the basic standards required for the construction of automobiles attracts a maximum penalty of one crore INR.[82] It is argued that the Indian consumer law should emphasize achieving the utmost welfare of the consumers and the state should adhere to preventive measures in order to ensure maximum consumer welfare, especially in the automobile industry. For example, the Central Government is statutorily empowered to recall such vehicles which can cause a potential loss to either

[76] Ibid, S. 42(4).
[77] Supra 37, S. 38 (2)(c).
[78] Ibid, S. 2 (6)(v).
[79] S. 16, The Prevention of Food Adulteration Act, 1954.
[80] Supra 67.
[81] *The Role of Prosecution in Consumer Protection*, The Australian Federation of Consumer Organizations INC., available at https://www.anu.edu.au/fellows/jbraithwaite/_documents/Articles/The%20role%20of%20prosecution%20in%20consumer%20protection.pdf, last seen on 06/11/2020.
[82] S. 182A (2), Motor Vehicles (Amendment) Act, 2019; See Rule 93, The Central Motor Vehicle Rules, 1989.

the environment or any other person on road, including the drivers.[83] Since the agencies certifying the compliance of the manufacturing standards are statutorily empowered and responsible to the government,[84] it shall act as a more proactive stakeholder in preventing any mishap with the consumers of the automobile industry.

Another criticism of the imposition of criminal sanctions in the continuously evolving automobile industry is that with the advancement of technology, it may be entirely impossible for the prosecution to prove, without doubt, that a particular manufacturer or distributor is at fault for producing a defective product.[85] Moreover, the Act stipulates that imprisonment shall also be levelled in cases where adulteration in a product does not cause any injury.[86] In such cases, there is no harm caused to the people at large, thus the gravity of punishment has to be likewise. It is suggested that a heavy compensation of 50 lakhs INR (or above) to the consumer along with a heavy penalty on the manufacturers and sellers, is required to be provisioned in the Act. In a few jurisdictions such as the USA, a fault-based liability is applicable, as per which, a manufacturer could be held under a deemed liability for designing a more risk-prone product (considering its foreseeable risks) that could be avoided by a less-risk-posing product.[87] But scholars have criticized its application on the grounds that the plaintiff consumers will not be able to successfully refute the design of the alleged products and produce a more effective product due to the lack of know-how of the industry standards.[88]

A deeper analysis of the Act reveals that the liability imposed therein, is in the nature of a no-fault liability which would be strictly applicable over the

[83] Ibid, S. 110A(1)(a); Supra 37, S. 20 (a) (The power to recall unsafe or hazardous products has been vested with the Central Consumer Protection Authority which has been established by the Central Government with effect from 24th July, 2020).
[84] Rule 126, The Central Motor Vehicle Rules, 1989.
[85] Thanuja Rodrigo, *Enhancing Sri Lankan Consumer Protection Through Consumer Guarantees and Strict Liability for Defective Goods-Lessons from the Australian Model of Consumer*, 21 Competition & Consumer Law Journal 165, 177 (2013) available at https://core.ac.uk/download/pdf/143889842.pdf, last seen on 07/11/2020.
[86] Supra 37, S. 90 (1) (a).
[87] Richard C. Ausness, *Product Liability 's Parallel Universe: Fault-Based Liability Theories and Modern Products Liability Law*, 74 Brooklyn Law Review 635, 654 (2009) available at https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1274&context=blr, last seen on 07/11/2020.
[88] Ibid, at 656.

manufacturers and sellers, predominantly. The liability accrues owing to the presumption that a product released in the market should be devoid of any potential harming element, and in case it is found to be harmful, the stakeholders are to be strictly held liable.[89] With the advent of criminal prosecutions in the Act and the standard of proof naturally being increased to that of 'beyond reasonable doubt', the pertinent question of successfully proving the guilt of the charged within a reasonable time needs deliberation. The authors are skeptical that long-run criminal trials would, in any circumstance, add to the relief of the consumers.

IV. CONSUMER PROTECTION FROM MISLEADING ADVERTISEMENTS

With the objective of effectively combating the issue of food and health safety in the country, the regulatory authorities resorted to cogent steps in order to ensure due prevention of any misleading information to the consumers and quick redressal in cases of losses suffered by such information.[90] The sincerity of their efforts became more evident when the government issued cautionary orders stipulating stringent directions to prevent the spreading of fake information.[91] Even the courts played a proactive role in preventing big corporations from misleading the public at large.[92]

---

[89] Alani Golanski, *Paradigm Shifts in Products Liability and Negligence*, 71 University of Pittsburg Law Review 673,682 (2010) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960619, last seen on 07/11/2020.

[90] *Food Safety and Standards Authority of India (FSSAI) Signs Mou with ASCI to Address Misleading Advertisements in the F&B Sector,* FSSAI, available at https://fssai.gov.in/upload/uploadfiles/files/Press_Release_MOU_ASCI_28_06_2016.pdf, last seen on 07/11/2020.

[91] *Order F. No. Z 25023 /09/2018-2020-DCC (AYUSH),* Ministry of Ayurveda, Yoga & Naturopathy, Unani, Siddha and Homoeopathy (AYUSH), available at https://www.ayush.gov.in/docs/121.pdf, last seen on 07/11/2020.

[92] Arudra Engineers Private Limited v. Patanjali Ayurved Limited, O.A.No.258 of 2020 and A.Nos.1532 & 1533 of 2020 in C.S.No.163 of 2020 (Madras High Court, 06/08/2020). Even though the plaintiffs filed a suit for trademark infringement against the defendants and the relief of injunction, as prayed was granted by the single bench of the High Court, the court on paragraph 126 observed, *"As stated above, there is no evidence that it is a cure for Coronavirus. Then most certainly coinage of the term 'Coronil' by the defendants is without due cause and in fact that intention to mislead the general public. They can always market the products, but they should be honest and declare that it is not a direct cure for Coronavirus, but rather an immunity booster. Usage of the word 'Coronil' and usage of the common pictorial image of Coronavirus are to put it very mildly, misleading and cannot be permitted and is therefore prohibited*". The order passed by the single bench disallowing the defendant Patanjali to continue using the name 'Coronil' was stayed by operation of an order passed by a division bench of the same high

The incorporation of a separate and wide definition of 'misleading advertisement'[93] in the Act as opposed to the issue being regulated as an unfair trade practice in the erstwhile legislation,[94] depicts a clear legislative intent to curb the exponential rise in the deceptive practices adopted by market competitors, which negatively influence consumer choices.[95] Moreover, the Act penalizes an incorrect or concealed narration of true facts, either through oral or written communications by a manufacturer or a service provider, with imprisonment extending up to two years and a liability amount extending up to fifty lakhs INR, in case of every subsequent offence.[96] These penalties can be levied by the statutorily formed Central Authority if, based on a complaint, it is necessary to do so and it appears to the Central Authority that a *prima facie* case exists against the manufacturer or an endorser with regards to a false or a misleading advertisement.[97] Here, it is argued that such grave penalties including criminal sanctions seem to be justified upon the manufacturers and dealers as their *mala fide* intention is patently reflected either through unreal promises or incorrect facts.

During 2008-15, the Volkswagen group in America claimed that its vehicles emitted low levels of nitrogen oxides, a major pollutant for environmental pollution than the permitted levels under the country standards. Its extensive advertising resulted in two separate actions initiated by the government's environmental agency and the justice department in the year 2016.[98] The evident reason was the sale of nearly five lakh fifty thousand vehicles across the country with emissions multiple times higher than existing standards. As a result, there were two major consequences. Firstly,

court and the Supreme Court of India refused to interfere with the judgment passed by the Division bench. In a case where the respondents were deceived regarding the affiliation of their prospective college, the Court also ordered for punitive damages, compensatory relief and necessary litigation costs to the aggrieved parties; See Buddhist Mission Dental College and Hospital v. Bhupesh Khurana, (2009) 4 SCC 484.

[93] Supra 37, S. 2 (28).

[94] Supra 1, S. 2 (1) (r) (2).

[95] Pushpa Girimaji, *Misleading Advertisements and Consumer*, 1 (1st ed., 2013).

[96] Supra 37, S. 89.

[97] Ibid, S. 21 (2).

[98] *FTC Charges Volkswagen Deceived Consumers with Its "Clean Diesel" Campaign*, Federal Trade Commission, available at https://www.ftc.gov/news-events/press-releases/2016/03/ftc-charges-volkswagen-deceived-consumers-its-clean-diesel, last seen on 08/11/2020.

consumers on a large scale were duped regarding the emission quality of the vehicles and, secondly, there was more damage to the environment than permissible under the laws.[99]

Therefore, it seems clear that misleading advertisements are willfully adopted tactics of the manufacturers or the endorsers in order to illegally gain an advantage by causing losses to the consumers. Criminal sanctions, thus, should be imposed on such corrupt and deceiving market influencers.

PART- II

V. PRODUCT LIABILITY UNDER CONSUMER PROTECTION ACT, 2019

1. The Early Origins of Product Liability

One of the earliest judicial precedents taught in the field of product-based liability remains that of *Carlill* v. *Carbolic Smoke Ball Co* ("**Carlill**").[100] In the time of an influenza epidemic in England, the case involved the sale of a "Smoke Ball" said to be effective in preventing the influenza flu. The advertising for the product promised a hundred pounds reward to anyone who used the ball as directed and still caught the flu. Carlill (the consumer) purchased the smoke ball and used it as directed but still managed to contract the influenza flu. In this case, the major question was whether a contractual relationship was established between Carlill (the consumer) and the Company, based on the advertisement alone.[101] Aside from the advertisement, there was no interaction between the Company and Carlill i.e., she was a "consumer" who purchased the smoke ball being sold in the retail market to anyone who would purchase it. Could the company be held

[99] Daniel Attas, *What's Wrong with "Deceptive" Advertising?*, 21 Journal of Business Ethics 49, 56 (1999) available at https://www.jstor.org/stable/pdf/25074154.pdf?refreqid=excelsior%3Ab2eaf58d74b558316f2adb1e499d8aa0, last seen on 09/11/2020 (By loss, the authors signify that moral culpability of the advertisers in hurting the sentiments of people who rely on such eye catching advertisements, and even if no personal/financial loss is suffered, the moral conscience of people in voluntarily making a choice does not remain independent and is not based on real facts and circumstances).

[100] Carlill v. Carbolic Smoke Ball Company, EWCA Civ 1(1892, Court of Appeal)

[101] Ibid, Bowen, L.J. "…It is also contended that the advertisement is rather in the nature of a puff or a proclamation than a promise or offer intended to mature into a contract when accepted. But the main point seems to be that the vagueness of the document shews that no contract whatever was intended."

accountable for promises made to prospective consumers in the advertisement, or was it a mere case of advertising gimmick?[102]

The Court held that a contractual relationship had in fact been established between the two parties. The fundamental requirements of a contract were fulfilled and there was a meeting of minds of the parties.[103] It meant that a consumer could be protected against a misleading and false advertisement and foundations for consumer protection were laid.[104] Therefore, while the case is significant from the perspective of contract law, it is also a significant early example relevant to consumer protection law, and a case from 1892 which is still good law in the United Kingdom being cited as recently as 2008.[105]

In Tort Law, *Donoghue* v. *Stevenson*[106] ("**Donoghue**") is another case that helped lay the foundations for the law of product liability. The case originated in Scotland where Ms. May Donoghue consumed a bottle of ginger beer and, while drinking it, noticed the presence of a dead snail inside the bottle. Falling sick from the consumption of the beverage, she brought an action against Stevenson (the manufacturer) in a court of law. It was claimed by May that the manufacturer, Stevenson, had a duty of care to ensure that the product was safe to consume (i.e., did not contain poisonous dead snails inside them).[107] May could not establish, however, that she had a contractual relationship with Stevenson or, in the absence thereof, that there was any legal duty of care owed by the manufacturer of

[102] Supra 100.
[103] Supra 100. "I cannot picture to myself the view of the law on which the contrary could be held when you have once found who are the contracting parties. If I say to a person, "If you use such and such a medicine for a week, I will give you 5l.," and he uses it, there is ample consideration for the promise."
[104] See Catherine Baksi*, Landmarks in Law: Louisa Carlill and the Fake Flu Cure,* The Guardian (25/6/2020), available at https://www.theguardian.com/law/2020/jun/25/landmarks-in-law-louisa-carlill-and-the-fake-flu-cure, last seen on 14/11/2020; Clive Coleman, *Carbolic Smoke Ball: Fake or Cure?,* BBC (5/11/2009), available at http://news.bbc.co.uk/2/hi/business/8340276.stm, last seen on 14/11/2020.
[105] Soulsbury v. Soulsbury EWCA Civ 969 (2007, Court of Appeal).
[106] A.C. 562 (1932, House of Lords); See Martin R. Taylor QC, *Mrs. Donoghue's Journey,* Scottish Law Reports, available at https://www.scottishlawreports.org.uk/resources/donoghue-v-stevenson/mrs-donoghue-s-journey/#one, last seen on 14/11/2020.
[107] Ibid. Ms. Donoghue's position is well explained in Martin R. Taylor QC.

a product to its consumers.[108] She also failed to establish that there was any negligence on the part of Stevenson in manufacturing the ginger beer.[109] Therefore the case failed in the first two instances.

This meant that the corpus of law and precedent as it stood at the time stood against May's path for legal remedy. In that regard, Lord Atkin's famous reasoning in *Donoghue* did not rest upon strictly legal principles and precedents but upon a conception of morality which might even seem vague in today's day and age.[110] His reasoning was based upon the moral principle that a person ought not to do harm to his neighbor which, when translated into legal terms, became the famed 'Neighbor Principle'.[111] He stated,

> The rule that you are to love your neighbor becomes in law, you must not injure your neighbor: and the lawyer's question, who is my neighbor? receives a restricted reply. You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbor. Who, then, in law, is my neighbor? The answer seems to be—persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question.[112]

So, the House of Lords went above and beyond existing law and precedent to give relief to the appellant. It meant extending the duty of care to an extent never recognized by courts before. The judgement remains a

---

[108] The failure to establish a contractual relationship was the reason that the case failed in Scottish Court of Appeal; See Ibid Martin R. Taylor QC. The reasoning was based upon the finding in Mullen v. A.G. Barr & Co. Ltd.; M'Gowan v. Barr & Co. S.C. 461 (1929, Court of Session) or the "mouse in the bottle case". That case was similar in fact to the present case, however in the absence of legal duty being established the case was ruled in favour of the manufacturers.

[109] Ibid. "The law of both countries appears to be that, in order to support an action for damages for negligence, the complainant has to show that he has been injured by the breach of a duty owed to him in the circumstances by the defendant to take reasonable care to avoid such injury. In the present case we are not concerned with the breach of the duty…"

[110] The moral and religious principles on which the Neighbour Principle was based is discussed in detail in Richard Castle, *Lord Atkin and the Neighbour Test: Origins of the Principles of Negligence in Donoghue v. Stevenson,* 7(33) Ecclesiastical Law Journal 210, 210 (2003), available at https://www.cambridge.org/core/journals/ecclesiastical-law-journal/article/lord-atkin-and-the-neighbour-test-origins-of-the-principles-of-negligence-in-donoghue-v-stevenson/CBCF36E5E5998EB037E232CAAE3317ED, last seen on 14/11/2020.

[111] Ibid.

[112] Supra 110.

landmark judgement in the law of tort. The first case found a contract where there was essentially none, and the second case did away with the requirement for a contract altogether.[113] In practical terms, both of these advanced the state of law at the time to make it simpler for consumers to get relief, when they were harmed by products they had purchased. Advancement of the state of law meant that more consumers could now approach the Courts for relief.[114] Therefore, these were important early steps in founding the law of consumer protection as it is known today. This advancement has also been linked to the technological revolution of the industrial revolution.[115]

2. The Development of the Doctrine of Strict Liability

In the USA, case law pronouncements further extended the protection of consumers as the doctrine of strict liability emerged in the 20th century. A combination of factors leading to the unique development of American consumer capitalism and changing social relations between the home and the manufacturers of goods is said to have necessitated the advancement of law to match it.[116] In the case of *Escola* v. *Coca Cola Bottling Co*[117] ("**Escola**"), the doctrine of strict liability for manufacturers in case of harm flowing from defects was pronounced. Arguably, the principle given in this case was equally as revolutionary as the one in *Donoghue*, and as time went on it was more or less directly incorporated into consumer protection laws around the world, including in India.[118]

Justice Traynor opined:

---

[113] F. Ferrari, *Donoghue v. Stevenson's 60th Anniversary,* 1(1) Annual Survey of International & Comparative Law 81, 84 (1994), available at https://digitalcommons.law.ggu.edu/annlsurvey/vol1/iss1/4/ last seen on 14/11/2020.
[114] Ibid, at 89. The case continues to "breathe new life" into the law of torts.
[115] As the means of production changed, newer forms of injury necessitated new legal pathways to remedy. The advancement of Tort Law was thus linked to the advancement of technology; Donald G. Gifford, *Technological Triggers to Tort Revolutions: Steam Locomotives, Autonomous Vehicles and Accident Compensation,* Journal of Tort Law (Forthcoming, 2018) available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090636, last seen on 14/11/2020.
[116] Supra 17, at 50. With the industrial revolution and development of railways, manufacturers of goods became remote from the home i.e., people no longer relied upon local handicrafts but on manufacturers whose factories were often located far away.
[117] Also known as the case of exploding glass bottles. Escola v. Coca-Cola Bottling Co. 24 C2d 453 (1944, Supreme Court of California).
[118] See the part on "Strict Liability Principles- An Effective Protection".

> In my opinion it should now be recognized that a manufacturer incurs an absolute liability when an article that he has placed on the market, knowing that it is to be used without inspection, proves to have a defect that causes injury to human beings.[119]

Twenty years later, the principle was tempered down from an 'absolute liability' to a 'strict liability' in *Greenman* v. *Yuba Power Products*[120] ("**Greenman**") by the very same Justice Traynor. In other words, the manufacturers will strictly bear the burden of liability but they would not be made liable under the garb of absolute liability.[121] The purpose of the principle of law established in *Escola* was clear: that the liability would have to be borne by manufacturers in case harm flows from their products. The reasoning given was based on both humanistic and economic concerns.[122] Firstly, it was noted that the consumers are in a considerably weaker position when it comes to inspecting the goods and checking for their safety before they are purchased. It is the responsibility of the manufacturers to ensure the safety of the articles, and that responsibility must be assumed by them at a higher degree than retailers and other intermediaries, even if it is not them who perform the task of checking, inspecting, and ensuring the safety of the products.[123] They are merely the intermediaries who relay the product to the consumers. Secondly, from an economic perspective, the manufacturers are most suited for liability because, by assuming the costs involved therein, they may suitably price the product, thereby distributing the costs back towards the consumers i.e., even though the manufacturers would assume the costs at the first instance, they would be distributed amongst the consumers finally.[124]

---

[119] Supra 117.

[120] Greenman v. Yuba Power Products, 59 Cal.2d 57 (1963, Supreme Court of California). As cited in GJ Adler, *Strict Products Liability: The Implied Warranty of Safety, and Negligence with Hindsight as Tests of Defect,* 2 Hofstra Law Review, available at https://scholarlycommons.law.hofstra.edu/hlr/vol2/iss2/9/, last seen on 15/11/2020.

[121] Ibid, GJ Adler 581. Absolute liability differs from strict liability in that not all harms flowing from a product would incur liability under strict liability.

[122] Supra 117. The following arguments are based on Justice Traynor's extensive explanations in *Escola.*

[123] Ibid. "*Manufacturing processes, frequently valuable secrets, are ordinarily either inaccessible to or beyond the ken of the general public. The consumer no longer has means or skill enough to investigate for himself the soundness of a product, even when it is not contained in a sealed package*."

[124] Supra 117. "*The cost of an injury and the loss of time or health may be an overwhelming misfortune to the person injured, and a needless one, for the risk of injury can be insured by the manufacturer and distributed among the public as a cost of doing business*."

From a legal point of view, the doctrine of strict liability made a significant contribution to the protection of consumers. Strict liability meant that neither privity of contract nor 'fault' based torts like negligence and misrepresentation would have to be proven in order for consumers to hold manufacturers liable.[125] The humanistic standard of *Donoghue* shined through once again, which was based on a much more general conception of duty on part of the manufacturers. Similarly, the requirement for privity of contract was discarded in an earlier case namely *MacPherson* v. *Buick Motor Co.*[126] The judgement in *Escola* showed a deliberate effort to sever the doctrine of strict liability from the law of contract and the doctrine of negligence in tort. It was finally recognized in this case that the variety of legal fictions would not be required to protect consumers under the doctrine of strict liability.[127]

The doctrine of strict liability in *Escola* and *Greenman* later spread across USA as consumer protection became more and more important.[128] Finally, in 1985, the EU too enacted the Council Directive 85/374/EEC,[129] introducing product liability based on a very similar language as the one used by Justice Traynor in *Escola.*[130] This led to the development of consumer protection laws in most other countries as well, including in

[125] Infra 140.

[126] In the United States, the requirement of privity of contract was done away with in the case of *Macpherson v. Buick Motor co.*, 217 N.Y. 382, 111 N.E. 1050 (Court of Appeals, New York).

[127] Supra 117. "In the food products cases the courts have resorted to various fictions to rationalize the extension of the manufacturer's warranty to the consumer: that a warranty runs with the chattel; that the cause of action of the dealer is assigned to the consumer; that the consumer is a third-party beneficiary of the manufacturer's contract with the dealer. They have also held the manufacturer liable on a mere fiction of negligence. Such fictions are not necessary to fix the manufacturer's liability under a warranty if the warranty is severed from the contract of sale between the dealer and the consumer and based on the law of torts."

[128] It was accepted into a majority of state jurisdictions in the United States and was later codified as S. 402A "SPECIAL LIABILITY"; Mathias Reimann, *Product Liability* 250, 251 in *Comparative Tort Law* (M. Bussani & A. Sebok, 1st ed., 2015).

[129] Council Directive 85/374/EEC of 25 July 1985 "on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products".

[130] Ibid, at 257. It has been argued that there is a "common core" of principles in the worldwide spread of product liability law. The influence of US case law on the development of product liability law is also discussed at length by the same author in Mathias Reimann, *Liability for Defective Products at the Beginning of the Twenty-First Century: Emergence of a Worldwide Standard,* 51(4) The American Journal of Comparative Law 751 (2003).

Eastern Europe, South America, and Asia.[131] However, product liability as such made an appearance in India only as late as 2019.

3. Product Liability Regime: The Indian Perspective

The Act codified product liability law for the first time for the Indian jurisdiction.[132] It is by no means, however, exclusively governing the field of product liability claims. A number of laws may be relevant for product liability, from the Indian Contract Act, 1872, the Sale of Goods Act, 1930, and the Indian Penal Code, 1860 to sector-specific laws like the Bureau of Indian Standards Act, 2016 ("**BIS Act**"), Food Safety and Standards Authority of India, 2006 ("**FSSA Act**"), Drugs and Cosmetics Act, 1940 and the Motor Vehicles Act, 1988.[133] Having previously discussed that the regime of warranties in contract and negligence were precluded by the introduction of the strict liability regime, we would not go into discussing those laws in this section. We have discussed the applicability of the criminal laws for consumer protection claims in detail in the previous section.[134] Therefore, in this section, we shall focus on the new provisions introducing product liability in the Act, with the intent to analyze the provisions in light of the development of the laws abroad, as has been seen above.

As for judicial development, before the introduction of the Act, there was no significant development with regard to strict liability.[135] Though English common law precedents related to tort law may have had some applicability, the principle of strict liability was not introduced through judicial pronouncement. In *Airbus Industrie* v. *Laura Howell Linton*[136]*,* the Karnataka High Court clarified that there is no law of strict product liability

[131] Supra 757.
[132] Majumdar & Partners, *Important Changes to India's Product Liability and Consumer Laws,* Lexology, available at https://www.lexology.com/library/detail.aspx?g=8a2ece1d-773a-4a51-bcd4-982d85a064c6, last seen on 14/11/2020.
[133] Amir Singh Pasrich & Amit Ranjan Singh, *In Brief: The Sources of Product Liability Law in India,* Lexology, available at: https://www.lexology.com/library/detail.aspx?g=22a07bfd-59dc-4772-8133-7f515a52f5ed, last seen on: 14/11/2020.
[134] See Section "Criminal Liability- An ineffective tool for consumer protection".
[135] A. Ghosh & N. C. Ray, *India: Product Liability Law In India: An Evolution,* Mondaq, available at: https://www.mondaq.com/india/dodd-frank-consumer-protection-act/974270/product-liability-law-in-india-an-evolution, last seen on 15/11/2020.
[136] Ibid., See Airbus Industrie v. Laura Howell Linton, ILR 1994 Kar 1370.

in India. The plaintiffs in that case, who were victims of an aircraft crash, were not allowed to prefer the USA jurisdiction for a product liability claim. The judges commented that,

> A mere fact that the Indian Courts does not have the strict product liability law, it is not wise to say that in such a situation and parties can go without any remedy. As it was done in *Charan Lal Sahu v. Union of India* (Bhopal Gas Disaster) that such antiquated acts can be drastically amended or fresh legislation should be enacted to save the situation.[137]

Relief came to consumers finally in the form of product liability in the Act.[138] The relevant sections of the Act introduce a comprehensive legal framework for assessing product liability claims by the Commissions empowered by the Act. While this paper has previously discussed some of the foundational cases that led to the introduction of product liability laws and the spirit that inspired them, the following discussion would consider some of the provisions of the Act based upon that standard. We would not go into the legalistic arguments but would rather analyze it in terms of the practical, social and economic impact that the law would have in action.

3.1 "Defects: Does the Law Expect too much from Consumers?

Product liability involves the *"claim for … any harm caused by a defective product."*[139] Undoubtedly, this is the language that was used in the *Escola* case and later again inspired the EU and UK laws as we saw in the previous section of this paper. For this purpose, the Act creates detailed provisions defining defects & deficiencies[140] and also a detailed procedure for proving the fact of the defect in such situations where alleged defects *"cannot be determined without proper analysis or test of the goods."*[141] This is followed by a lengthy process of sending defective goods for independent analysis, followed by a procedure for the parties to dispute the conclusions of the independent laboratory.[142] Decisions of the National Consumer Dispute Redressal Commission (**"NCDRC"**) also indicate the burden of proof,

[137] Ibid.
[138] See Chapter VI on "Product Liability", The Consumer Protection Act 2019.
[139] Supra 37, S. 82.
[140] Ibid, Ss. 2(10) & 2(11).
[141] Supra 37, S. 38(2).
[142] Ibid, Ss. 38(2)(c)-(g).

ordinarily, being upon the one who alleges the defect.[143] Indeed the standard followed by the NCDRC, at least before the implementation of the Act, was closer to negligence than strict liability.[144] In other decisions, the principle of *res ipsa loquitur* was followed.[145]

The very first question we ask involves whether the Act, as codified law, provides adequate clarity about the burden of proof with regards to the defect in product or service. Does the burden of proof lie upon the complainant or is it the manufacturers who have to answer for the harm caused by the use of their goods in a reasonable manner? Indeed, there are a number of alternative theories which may be relevant in deciding this question.[146] There are indications that 'strict liability' of the *Escola* type fell out of fashion in the USA by the 1980s, as Courts reverted to a negligence-based standard.[147] *Escola* seemed to indicate that the claimant just has to prove that in the ordinary and reasonable use of the product, he has bought placing his faith upon the name of the manufacturer, harm has befallen him from the product itself. Whereas, the standard demanded in the Act could be reasonably interpreted as demanding direct proof of defect and its co-relation to the damage suffered by the claimant.[148]

Is it a betrayal to the spirit of *Escola?* As manufacturing processes get more technical, complicated, and secretive, we do not think it can be reasonably expected for an ordinary consumer to establish defects in the process of manufacturing known only to the manufacturer himself (or otherwise, for

[143] Jai Prakash Verma v. J.K. Lakshmi Cement Ltd, (2013) CPJ 54 (NC).
[144] "It is well acknowledged crystallized by a catena of decisions that mere loss or injury without negligence was not contemplated by section 14(1)(d) of CP Act, 1986 …." as held in Madhusudhan Rao v. Air France, Revision Petition No. 3792 of 2008 (NCDRC, 01/04/2010).
[145] In the case of a child losing her life because of a poorly maintained escalator by the Airport Authority, the doctrine of *res ipsa loquitur* was allowed in Geeta Jethani v. Airports Authority of India III, 2004 CPJ 106 NC.
[146] Three approaches taken by Courts in US product liability are mentioned as: 1) The direct proof method, where direct proof and expert testimony were required to show a direct correlation between the defect and the damage caused. 2) The *Res ipsa loquitur* method where defect would be inferred by circumstantial evidence 3) Where showing that the product did not perform as expected was enough; DS Niss, Products Liability: Methods of Pleading and Proof for the Plaintiff, 49(1) North Dakota Law Review 105, 109 (1972), available at https://commons.und.edu/ndlr/vol49/iss1/7, last seen 15/11/2020.
[147] Supra 126 at 53.
[148] Infra 154.

services).[149] It can also be said that the process itself imagined in the Act, gives too much leverage to the manufacturers or other persons to influence the procedure of establishing defects.[150] It has to be remembered that, ordinarily, manufacturers are vastly more empowered than ordinary consumers, and the Commission has to determine whether the claim of the complainant is genuine or not; without going into too much detail about the 'fault' of the manufacturers of the product or service in question. Relieving complainants from undue burden in proving the fault of manufacturers in such situations would perhaps be more in the interest of consumer protection.[151] Fault-based liability is the realm of negligence law, whereas strict liability was brought in to do away with the complications of proving faults on the part of the manufacturers.[152] Therefore, it is argued that manufacturers should be strictly liable for the losses caused to the consumers in order to maintain the power balance between them and the manufacturers, as well as relieving the complainants/consumers from the difficulty of proving the liability of the wrongdoers.

3.2 The Liability of Third Parties: Clarity Required!

Now the Act provides for product liability claims to be filed against 'manufacturers, product sellers or product service providers'.[153] In *Escola*, considerable discussion was dedicated to the reason behind affixing liability upon the manufacturer himself.[154] The first reason is the economic one, that by making producers liable, they are able to distribute the costs of liability to the end consumers themselves by pricing the products higher.

---

[149] Supra 117. "*As handicrafts have been replaced by mass production with its great markets and transportation facilities, the close relationship between the producer and consumer of a product has been altered. Manufacturing processes, frequently valuable secrets, are ordinarily either inaccessible to or beyond the ken of the general public. The consumer no longer has means or skill enough to investigate for himself the soundness of a product, even when it is not contained in a sealed package, and his erstwhile vigilance has been lulled by the steady efforts of manufacturers to build up confidence by advertising and marketing devices such as trade-marks.*"

[150] Infra 154.

[151] Supra 132.

[152] Supra 139.

[153] Supra 37, S. 2(6)(vi).

[154] Supra 117. "*The manufacturer's obligation to the consumer must keep pace with the changing relationship between them; it cannot be escaped because the marketing of a product has become so complicated as to require one or more […] intermediaries. Certainly, there is greater reason to impose liability on the manufacturer than on the retailer who is but a conduit of a product that he is not himself able to test.*"

Indeed, it is the manufacturers who authorize others like wholesalers and dealers to bring the products to the consumers.

Here, it is important to consider the position of the producer of the goods with regards the intermediaries of the product.[155] In the process of production, a manufacturer has to consider carefully from where and at what cost and quality he would acquire the materials and components which are used in the final product. He has to decide who would be authorized to act as intermediaries between him and his consumers as well, i.e., he enters into careful considerations about the entire supply chain. If he gives up any aspect of control over the production of the goods, it is at his discretion, and establishing where the 'fault' lies in causing the defect and affixing the liability is an exercise which would only lengthen proceedings excessively when, it is the producers who are responsible in bringing the elements together and managing the supply chain of the product. Consequently, the consumer relies upon the brand value of and advertisements by the producers, rather than that of the intermediaries, while purchasing a product.[156]

Making reference to the language of the EU Directive,[157]

> Whereas liability without fault on the part of the producer is the sole means of adequately solving the problem. Whereas the protection of the consumer requires that the liability of the producer remains unaffected by acts or omissions of other persons having contributed to cause the damage; whereas, however, the contributory negligence of the injured person may be taken into account to reduce or disallow such liability.

There is considerable emphasis on the liability being fixed primarily upon the producers who have affixed their brand name upon the product. Evidently, the NCDRC has also preferred this approach in the past.[158]

---

[155] The intermediaries are the wholesalers, retailers, distributors, service providers and others who bring the product to the consumer.

[156] Supra 117. "…his (consumer's) erstwhile vigilance has been lulled by the steady efforts of manufacturers to build up confidence by advertising and marketing devices such as trade-marks. Manufacturers have sought to justify that faith by increasingly high standards of inspection and a readiness to make good on defective products by way of replacements and refunds."

[157] Supra 32.

[158] There is a line of cases which provide for the liability of the manufacturer in cases of product liability. See Hind Motors India Ltd. v. Jodh Singh 2016 (3) CPR 35; Rama

Although the liability under a product liability action is primarily based on a product's manufacturer or its seller, the latter's definition under the Act is comprehensive to include various intermediaries like distributors and installers, amongst others.[159] Thus, it can be inferred that a wide definition would encompass similar intermediaries such as transporters, though any binding precedents in the future would make the liability more unambiguous.

The spirit of justice that brings relief to the masses of people was what brought *Donoghue* and *Escola* and other landmark cases to their prominent positions in the laws of the countries where they were written. These were cases that went far beyond existing law and precedent in order to bring relief to those who came to the Courts seeking justice. It is therefore completely understandable why the principles in these cases could not stay confined to their home jurisdictions, but spread across the world and became famed. In that light, we tried to analyze the introduction of product liability in the Act. Certainly, extensive efforts have been made to create comprehensive legislation and the Act provides an up-to-date framework to deal with cases of product liability. That being said, we found that the Act could have done more to provide adequate clarity over the technicalities of product liability law. Some of the provisions could indeed be interpreted in a way that doesn't do justice to the spirit of consumer protection law and may end up placing an undue burden over claimants in the consumer forums. Whereas we have discussed the aspect of the standard of defects and the liability of intermediaries in this light, more aspects like contributory negligence of complainants,[160] and the applicability of special laws in regard to product liability[161] may be explored

Shankar Yadav vs. J.P Associate Ltd. (2012) CPJ, 110 (NC); Mantu Chandra Roy v. The Proprietor of Great Eastern Trading Co. (DCDRC Decision, 2018).

[159] Supra 37, S. 2(37).

[160] Supra 132 at 599.

[161] Supra 145. Special Laws overlap with the Consumer Protection Act 2019 in providing a remedy for defective products. These laws contain provisions for recall of products and may become relevant in cases where defective products have been sold *en masse* to consumers and must be recalled by the companies in question. These laws may also impose other requirements on manufacturers. For an introductory discussion, refer to V. Bajaj, K Raghavan, S. Kaul, *India: Product Liability Laws and Regulations 2020*, ICLG, available at (https://iclg.com/practice-areas/product-liability-laws-and regulations/india), last seen on 15/11/2020.

more deeply. Finally, it is also worth exploring the conditions for product liability law to succeed exist in India.[162] However, it can be reasonably expected that product liability law would become more important as India further develops economically and as technology plays a bigger role in the lives of people.

PART- III

VI. REGULATING ARTIFICIAL INTELLIGENCE UNDER INDIAN CONSUMER LAW: A FORESEEABLE FUTURE OR A DISTANT REALITY?

In the last decade, numerous efforts have been made in the field of AI and future technology and its effect on society at large: from doomsday predictions over the rise of autonomous machines and 'war-robots',[163] to concern over the rise of BigTech giants and their exceeding leverage over society.[164] Indeed, we are seeing a greater role of machines in carrying out processes which were earlier thought only possible by human beings and, therefore, a greater role of machines in our day-to-day social, economic and cultural lives, especially for the consumers. A popular example is that of the hassle-free recommendations of the YouTube videos based on prior utilization of consumers' time on that giant platform.

As per the recent statistics released by Oxford Insights and the International Research Development Centre (**"IDRC"**), India has been

[162] Supra 140 at 810. The law of product liability is far more developed in the United States than any other jurisdiction in terms of the number of cases, the size of awards, class-action suits, and other factors including the amount of publicity any particular case may get. Further, factors like industrialization and the advancement of consumer capitalism are also linked to the development of product liability law.

[163] The development of fully autonomous robots designed to make war may not be very far away technologically. These machines may be programmed with the capability to break the fundamental rules which govern robots and thus go "terminator"; See DC Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 Wash. L. Rev. 117, 123 (2014), available at https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4800&context=wlr, last seen on 13/11/2020.

[164] See E Mik, *The Erosion of Autonomy in Online Consumer Transactions,* 8 Law, Innovation and Technology 1 (2016), available at https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3688&context=sol_research, last seen on 15/11/2020.

ranked 40th in terms of its government's readiness to adopt AI,[165] with primary areas of focus to be infrastructure and access to high-quality data.[166] Although the term AI has been related with different connotations[167] highlighting the importance of the concept, the Hon'ble Prime Minister of India has taken a leap ahead and referred to AI as a tribute to human intellectualism in the recent RAISE 2020 summit hosted by the nation.[168] Such praise can be justified due to the achievements possible owing to AI technology.[169] But what does AI mean? Broadly, AI refers to the use of algorithmic combinations to prepare automated systems that can perform different tasks based on self-recommendations and thinking.[170] Such independent compositions (often called robots) can not only effectively demonstrate the use of AI but are often found to be friendly companions to humans.[171]

The existing literature on AI shows that there is a continuous evolution in the field[172] which leads lawmakers around the globe to cogitate about the possibilities of recognizing and entitling such systems with rights and duties

---

165 *Government AI Readiness Index 2022*, Oxford Insights, available at https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/5f7747f29ca3c20ecb598f7c/1601653137399/AI+Readiness+Report.pdf, last seen on 10/11/2020.

166 Id, at 99.

167 See *Smart Strategy Turns AI into Action*, Accenture, available at https://www.accenture.com/in-en/services/ai-artificial-intelligence-index, last seen on 12/11/2020; *Artificial Intelligence (AI)*, IBM, available at https://www.ibm.com/cloud/learn/what-is-artificial-intelligence#toc-what-is-ar-DhYPPT4m, last seen on 13/11/2020.

168 *"Artificial Intelligence is a Tribute to Human Intellectual Power," Prime Minister Narendra Modi*, IndiaAI, available at https://indiaai.gov.in/article/artificial-intelligence-is-a-tribute-to-human-intellectual-power-prime-minister-narendra-modi, last seen on 12/11/2020.

169 *This AI Can Identify The Coughs Of Asymptomatic People With Covid-19*, Mashable India, available at https://in.mashable.com/tech/18015/this-ai-can-identify-the-coughs-of-asymptomatic-people-with-covid-19, last seen on 13/11/2020.

170 *CCBE Considerations on the Legal Aspects of Artificial Intelligence*, Council of Bars and Law Societies of Europe, available at https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf, last seen on 13/11/2020.

171 Dilip V. Jeste et al., *Beyond Artificial Intelligence: Exploring Artificial Wisdom*, 32 International Psychogeriatrics 993, 997 (2020), available at https://www.cambridge.org/core/services/aop-cambridge-core/content/view/AEFF76E8D643E2B7210995E3ABDAA722/S1041610220000927a.pdf/beyond_artificial_intelligence_exploring_artificial_wisdom.pdf, last seen on 14/11/2020.

172 Olivia Cuthbert, *Saudi Arabia Becomes First Country to Grant Citizenship to a Robot*, Arab News (26/10/2017) available at https://www.arabnews.com/node/1183166/saudi-arabia, last seen on 14/11/2020.

as applicable to *homo sapiens*.[173] Although in some jurisdictions, limited use of AI technology is prevalent, the absence of legislation governing such systems calls for a discussion.[174] Under the Indian consumer protection law, however, the inclusive definition of the term 'person' to include an artificial juridical person[175], has widened the debate for imputing liability but the imputation still remains far from reality. The reason is that the liability for a default in a good or service can only be attached to a real human being, may it be its manufacturer, seller, and an artificial system remains far from being liable for any harm caused to a consumer. Furthermore, the Act does not envisage the imposition of liability over a networking system or any intermediary technological advancement in manufacturing a product, rather the creator of the product itself.[176]

However, before stipulating liabilities, it is imperative to possess a codified mechanism that can regulate AI. In the Indian context, the discussion paper on National Strategy for AI highlights that sector-specific reforms, along with comprehensive participation of the different stakeholders with effective control of the government, are required for the country to emerge as a leader in the field of AI.[177] The said paper identifies *inter alia* core research, lack of infrastructure, and unawareness of AI technology as the underlining challenges in the AI field in India.[178] Other related issues involve the use of data in AI systems and the lack of legal personality of AI.[179] Thus, with ongoing research and analysis of the different policy

[173] Simon Chesterman, *Artificial Intelligence and the Limits of Legal Personality*, 49 ICLQ 819, 820 (2020), available at https://www.cambridge.org/core/services/aop-cambridge-core/content/view/1859C6E12F75046309C60C150AB31A29/S0020589320000366a.pdf/artificial_intelligence_and_the_limits_of_legal_personality.pdf, last seen on 14/11/2020.

[174] *Liability for Artificial Intelligence and Other Emerging Digital Technologies*, European Commission, available at https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608, last seen on 14/11/2020.

[175] Supra, 37, S. 2 (31) (vii).

[176] Ibid, S. 2 (36).

[177] *National Strategy for Artificial Intelligence# AI For All*, IndiaAI, available at https://raise2020.indiaai.gov.in/src/images/pdf/NationalStrategy-for-AI-Discussion-Paper.pdf, last seen on 14/11/2020.

[178] Ibid, at 46.

[179] Chris Reed, *How Should We Regulate Artificial Intelligence*, Phil. Trans. R. Soc. A 1, 4 (2018), available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6107539/pdf/rsta20170360.pdf, last seen on 14/11/2020.

issues related to AI, in this part, it is attempted to explore the different liability regimes with respect to AI and seek to contribute valuable inputs in this emerging field.

1. Early Conflicts and Controversies

Whether the fears would become real or not, we are yet to see. The beginning of legal action against Big Tech, however, has begun with cases creeping up from different jurisdictions. In Australia, the 'Robodebt scandal' is an early example of how algorithm-based AI led to a financial scandal where hundreds of thousands of people were affected.[180] Robodebt here refers to an automated debt collection system created to collect debt on behalf of the Government of Australia.[181] The system would compare the financial data of individuals to calculate the 'robo-debt' they owed based on discrepancies in their financial data. The system went from being semi-automated in 2011 to fully automated by 2016.[182] As a result, false debt notices were sent to hundreds of thousands of people who went through the harrowing process of contesting numbers calculated by a machine.[183] Finally, the Australian Government was forced to take back the Robodebt scheme and pay back the individuals whose debt was wrongly calculated.[184]

The scandal is an early example of how AI-driven automated decision-making systems can lead to discrepancies and cause harm to ordinary citizens.[185] These types of systems are now being used for diversified tasks:

---

[180] LH Gomes, *Robodebt: Government to Refund 470,000 Unlawful Centrelink Debts Worth $721m,* The Guardian (29/05/2020), available at https://www.theguardian.com/australia-news/2020/may/29/robodebt-government-to-repay-470000-unlawful-centrelink-debts-worth-721m, last seen on 15/11/2020.

[181] For a detailed report on the Robodebt system, See Gillian Tersiz, *Austerity is an Algorithm,* Logic (01/12/2017), available at https://logicmag.io/justice/austerity-is-an-algorithm/, last seen on 15/11/2020.

[182] Ibid.

[183] Supra 181.

[184] Supra 181. It has presently become the subject of a class-action suit against the Government of Australia, See *Centrelink Robodebt Class Actions Lawsuit to be Brought Against the Federal Government*, ABC News (17/09/2019), available at https://www.abc.net.au/news/2019-09-17/centrelink-robodebt-class-action-lawsuit-announced/11520338, last seen on 15/11/2020.

[185] There's a difference between Decision Making System and Decision Supporting System, specifically, in the degree of autonomy that the system has. Decision making systems may be authorised to process information and also to initiate further actions by themselves. See *The Difference Between Decision Support Systems and Decision Management Systems*

from automating administrative tasks, human resources and recruitment decisions to making complex human predictions.[186] There are other more controversial uses of such systems too, for example, in profiling criminal offenders and assessing the likelihood of repeat offenses.[187] From being profiled for one's political or religious views by automated systems on social media, to financially profiled or credit-rated, they may help or harm their human targets. On the other hand, the same data may be used by corporations to profit off the very same consumers by carefully targeted advertising.[188]

Thus, comes a second concern over the role of Big Tech in our day-to-day lives: data privacy.[189] When it comes to data, it seems that everyone wants a slice of that pie. Data is equally valuable for governments,[190] as it is for corporations,[191] and for intellectuals who may wish to understand better how human beings act and think. But what about the users themselves? As we have already waived the rights to our data to major corporations, what if we wish to sign off? An important concern raised in Italian Corporate & Consumer Authority against the 2016 WhatsApp-Facebook merger was that after the merger of WhatsApp and Facebook (which were already

for Decision Automation, James Taylor, available at http://www.decisionmanagementsolutions.com/the-difference-between-decision-support-systems-and-decision-management-systems-for-decision-automation/#:~:text=Decision%20Management%20Systems%2C%20unlike%20Decision,the%20actions%20to%20be%20taken, last seen on 15/11/2020.

[186] UNHCR Innovation Service, *7 Ways You Can Automate Decision Making for Good,* Medium, available at https://medium.com/unhcr-innovation-service/7-ways-you-can-automate-decision-making-for-good-14005fedf6a5, last seen on 15/11/2020.

[187] Ibid. See *COMPAS,* State of Wisconsin-Department of Corrections, available at https://doc.wi.gov/Pages/AboutDOC/COMPAS.aspx, last seen on 15/11/2020. The system is criticised for systematic biases.

[188] For an excellent documentary on the same See *The Social Dilemma*, Netflix, available at https://www.netflix.com/search?q=The%20social%20dilemma&jbv=81254224"Netflix", last seen on 15/11/2020.

[189] See section on "Regulated Autonomy" in A. Jabłonowska, M. Kuziemski, AM Nowak, HW Micklitz, P Pałka & GSartor, *Consumer Law and Artificial Intelligence: Challenges to the EU Consumer Law and Policy Stemming from Business' Use of Artificial Intelligence- Final Report of the ARTSY Project,* EUI Working Paper LAW 2018/11, European University Institute 12 (2018).

[190] Two methods governments may access private data include direct access into private-sector databases without intervention of the service providers and access with the intervention of service providers. See IS Rubenstein, GT Nojeim & RD Lee, *Systematic Government Access to Personal Data: A Comparative Analysis,* 4(2) International Data Privacy Law 96 (2014).

[191] Advertising revenues from data are said to be considerable. On the other hand, social media companies may be able to improve User Experience through more and more data. Supra 173.

instant messaging giants before the merger),[192] Facebook would have access to the data of even those persons who were not Facebook users but only users of WhatsApp.[193] Privacy concerns are, thus, exacerbated by the recent mergers of data giants like Facebook-WhatsApp-Instagram & YouTube-Google.[194]

In light of this, it is understandable why considerable interest is being generated in the USA to break up these companies.[195] While the arguments against these corporations are based on competition laws, data rights and consumer rights are also important factors that underpin these actions because these difficulties only arise due to extensive consumer data accumulation on the part of social media giants.[196] Political interference and manipulation from social media platforms has also been a concern, especially after the Cambridge Analytica Scandal.[197] These concerns were raised again in the 2020 US General Elections, where it was alleged that major social media companies had themselves played an unlawful role of 'censoring' content belonging to one political group.[198] Whether the allegations are true or not, it is beyond doubt that social media giants certainly have the wherewithal to unilaterally interfere in political processes without any requirements for transparency or accountability to their

[192] For a full review of the case, See N Zingales, *Between a Rock and Two Hard Places: WhatsApp at the Crossroad of Competition, Data Protection and Consumer Protection Law,* Computer Law and Security Review (2017).
[193] LB Moses, *Recurring Dilemmas: The Law's Race to Keep up with Technological Change,* 4 (2017), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=979861, last seen on 15/11/2020.
[194] Ibid.
[195] Matt Peterson, *For Tim Wu, Breaking Up Facebook is Just the Beginning,* The Atlantic (28/01/2019), available at https://www.theatlantic.com/membership/archive/2019/01/for-tim-wu-breaking-up-facebook-is-just-the-beginning/581485/, last seen on 15/11/2020; See Kaitlyn Tiffany, *A simple plan to dissolve Facebook, Google, and Amazon*, Vox (8/11/2018), available at https://www.vox.com/the-goods/2018/11/8/18076440/facebook-monopoly-curse-of-bigness-tim-wu-interview, last seen on 15/11/2020.
[196] Supra 192. These issues exist at the "crossroads of competition, data protection and consumer protection law." Italian authorities found numerous consumer rights and data privacy violations in the act of WhatsApp changing their Terms of Service unilaterally after the merger with Facebook.
[197] See Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening,* Wired 17/03/2019, available at https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/, last seen on 15/11/2020.
[198] *Facebook, Twitter Accused of Censoring Article Critical of Biden,* The Times of India (15/10/2020), available at https://timesofindia.indiatimes.com/world/us/us-presidential-elections/facebook-twitter-accused-of-censoring-article-critical-of-biden/articleshow/78672510.cms, last seen on 15/11/2020.

consumers or the society at large. The usual defense to allegations of malpractice by social media giants has been that they are mere 'platforms' that do not interfere in the content posted by their users.[199] However, they have a proven capacity to manipulate traffic on their websites,[200] and therefore, there are increasing calls to treat social media giants as 'publishers' rather than 'platforms'.[201]

That may still be a long way ahead as lawmakers, academics, and commentators try to piece together a narrative that makes sense while balancing concerns on either side of the dichotomy.[202] As it stands, consumers of the services do have certain important rights that must be kept in mind. For example, the 'right to be informed', the 'right to awareness' and the 'right to seek redressal against unfair trade practices'.[203] As for personal data rights, the Personal Data Protection Bill, 2018 does include extensive rights for the protection of users.[204] At the preliminary stage, it may be questioned why such extensive procedural requirements for a person to delete his own personal data under the 'Right to be Forgotten'[205] are justified. In the dichotomy of corporations and regulators, a third nix is thereby added: the individual (user or consumer). Without any

[199] Platforms have a lesser regulatory burden as compared to publishers. This sort of concession is available in India as well under Section 79-II of the Information Technology Act, 2000. Though the demand for more regulation for social media giants is increasing. See *In the United States:* Adam Candeub, *Social Media Platforms or Publishers? Rethinking Section 230*, The American Conservative (21/06/2019), available at https://www.theamericanconservative.com/articles/social-media-platforms-or-publishers-rethinking-section-230/, last seen on 15/11/2020; *In India:* AS Mankotia & A Chaturvedi, *New Clause added to IT Act: Onus of Content not Generated by users on social media platforms,* The Economic Times 07/02/2020, available at https://economictimes.indiatimes.com/tech/internet/new-clause-added-to-it-act-onus-of-content-not-generated-by-users-on-social-media-platforms/articleshow/73996954.cms?from=mdr, last seen on 15/11/2020

[200] Supra 173.

[201] Supra 199.

[202] Supra 201.

[203] Supra 37, S. 2 (9). Generally, rights of this type are available in most consumer protection legislations around the world including in India.

[204] See Chapter V, The Personal Data Protection Bill, 2018.

[205] "The data economy" right now is like a door once opened that cannot be closed again; once we are plugged in, we are irreversibly trapped in the system. It is questionable why one would need to approach the Data Authority for being removed from the online world if one so wishes. See "Right to be Forgotten", S. 27(2), Personal Data Protection Bill, 2018.

definitive 'right to ownership of personal data',[206] it does not seem that the individual would win any time soon.

2. Imposing Liability on AI Systems and Robots

The previous research in the AI field shows that the opinion on imposing criminal liability is muddled. One section of scholars think that at some point in the future, criminality can be analyzed vis-à-vis AI machines, but presently there is no such scope.[207] Although the thinkers in this line of though agree that the mental element is nearly unsatisfied in all the suggestive models of imposing criminal liability,[208] they are keen to use the 'natural probable consequence model' to argue that even the unintended or undesired consequences of the technological inputs in the machines should make the liability vest on the machines.[209] We think that this approach is totally miscalculated on multiple grounds. Firstly, it overlooks the possibility of the machine malfunctioning and attributes the liability merely to the consequences. Secondly, it completely neglects the mental framework of emotions and feelings fed to the machine, which can lead the machine to act in a defensive manner or out of several compulsions.[210] The other opinion is that if any harm is caused by a morally conscious

[206] There is considerable hesitation over recognition of a right to ownership of personal data. Arguably, it is not the ownership of personal data that is in question but rather the temporary access given by an individual to certain data which they should hypothetically be able to take back at any time. See CF Kerry, and JB Morris Jr., *Why Data Ownership is the Wrong Approach to Protecting Privacy,* Brookings (26/6/2019), available at https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/, last seen on 15/11/2020.

[207] Supra 172 at 124.

[208] Gabriel Hallevy, *The Criminal Liability of Artificial Intelligence Entities*, 1, 23 (2010), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1564096, last seen on 14/11/2020. (Out of the three models for imposing criminal liability suggested by Professor Gabriel, which are perpetration by another liability model, natural probable consequence liability model and direct liability model, none argue, even remotely, that a mala fide intention can be bestowed upon the AI systems, without which no criminal liability can be imposed upon either an AI system or robots. Here, it needs to be clarified that the imposition of criminal liability on AI systems is to be separately dealt with that of either its programmer or an identified user, which according to Professor Gabriel, are the liable stakeholders for imposing criminal liability).

[209] Gabriel Hallevy, *I, Robot - I, Criminal: When Science Fiction Becomes Reality: Legal Liability of AI Robots Committing Criminal Offenses*, 22 Syracuse Sci. & TECH. L. REP. 1, 14 (2010).

[210] See Chapter IV "General Exceptions", The Indian Penal Code, 1860. (If an AI built machine or a robot is found to act under any of the defences available under domestic and global criminal laws, then such act should be exempted from liability).

robot, it may be held liable and not otherwise.[211] To elaborate, the proponents of attributing criminal liability assume that the AI system is aware of the wrongs that it commits and does not merely perform the act with an intention to fulfil the directions given by the system manufacturer.[212]

Under the Indian context, it appears to us that to attribute any form of liability to AI systems, it is imperative to define the systems under the definition clauses in the law. While the Indian criminal law is sufficiently wide to include AI systems within its applicability,[213] there is no such provision in modern consumer legislation. Notably, the Act delves into a limited discussion regarding a product's design, and not its internal components,[214] thereby limiting the scope to a product's appearance and usage, instead of the inbuilt mechanism. Moreover, the existing challenges in the AI industry, including that of infrastructure and access to tech-knowledge have to be conquered prior to establishing a criminal sanction on an AI system.

3. Strict Liability Principles: An Effective Protection?

Challenges regarding the role of Big Tech in our lives, the necessity of innovation, the regulation thereof, and the importance of the rights of individuals are without any clear answers yet. The process of social churning with the pull and push of different sides is continuously going on in this fast-evolving realm. In the meantime, we may wonder whether the existing legal machinery we have at hand yields the principles of law that may serve to effectively protect the general public from the dangers of future technology.

The question was dealt with extensively by Vladeck in Machines Without Principals: Liability Rules and Artificial Intelligence.[215] He argues that the

[211] Ying Hu, *Robot Criminals*, 52 U. Mich. J. L. 487, 512 (2019), available at https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1806&context=mjlr, last seen on 14/11/2020.
[212] Ibid, at 522.
[213] S. 11, The Indian Penal Code, 1860.
[214] Supra 37, S. 2 (12).
[215] Supra 173.

principles of strict liability[216] may be able to provide an effective remedy for consumers of future technologies, while acknowledging that manufacturers may be able to escape liabilities because of the even more complicated relation between manufacturers and suppliers of components in case of future technologies. For any harm caused to consumers, the question asked is 'who pays?'. How would liability be apportioned amongst the many different parties involved in designing, testing, manufacturing these vehicles?[217] Personally, for reasons stated in the earlier section, it is believed that it is the manufacturer who is to be primarily held liable. This is on account of the immense reputation carried by the manufacturers, who are presumed to have tested the nitty-gritties of a product before launching it in the market. Certainly, after procuring the services of every component manufacturer, designer, part engineer, software engineer and others, the manufacturer adds a significant dividend to the costs as profits for himself. So, it is believed by us that the primary liability in case of harm caused by defects should primarily be borne by the manufacturer himself. Here, the view that liability, if any, imposed on the AI systems instead of the manufacturers will benefit the consumers is outrightly rejected on dual grounds. Firstly, being purely mechanical in nature, AI systems will not be able to address consumer grievances, in terms of providing compensation for the latter's losses or even assuring them better future performance. Secondly, being bereft of human emotions, AI systems may not be able to comprehend the real and pressing predicaments of the consumers. For instance, the consumers' demand for a specific quality product may not be addressed by an unnatural system such as AI.

In light of cases such as *Donoghue* and later *Escola,* where there is a genuine case of harm, the barriers towards legal redressal and remedy should be minimized as much as possible.[218] Practically, the legal mechanism can itself become the barrier to justice but, in those cases, an example was set whereby a very general and humanistic principle was applied in order to

[216] Supra 173 at 146.
[217] Supra 173 at 128.
[218] RJ Currie, *Of Neighbours and Netizens, or Duty of Care in the Tech Age: A Comment on Cooper v. Hobart*, 3(2) Canadian Journal of Law and Technology 81, 87 (2004), available at https://ojs.library.dal.ca/CJLT/article/viewFile/6095/5414, last seen on 15/11/2020.

provide justice even where no previous law would be able to deliver it. It seems to us that, it is the spirit that runs through the doctrine of strict liability and the codified regimes of product liability which are based thereupon.

Thus, while there is still a legal vacuum in regulations of advanced systems such as AI & robotics around the world, it appears that the doctrine of strict liability over manufacturers and producers of all products and services including AI systems could prove to be an effective means for combating the liability issue, in cases of harm caused to the consumers.

VII. CONCLUSION

With a continuous increase in the investment opportunities in the consumer industry, the emerging technology and stiff competition amongst the market-dominating stakeholders leads to new challenges for legislators across the globe. The enactment of a reformed legislation by the Indian Parliament seeks to enforce a stronger deterrence and overcome the problems posed by the enforcement of the erstwhile consumer law. In Part 1 of this paper, the examples of prevalent consumer laws in China and the USA helped to understand the consumer grievance models based on heavy compensation and criminal sanctions, though each model remains heavily critiqued by the domestic scholars and it is inferred that neither model can adequately address the delay under the Indian procedure. In the Indian context, although the criminal law applies extraterritorially, having the potential to hold different stakeholders including manufacturers, retailers, sellers, and distributors criminally liable, the same shall not prove to be an effective tool for consumer protection, especially in the automobile industry, for multiple reasons. It must be noted that, since this industry has the potential to include stakeholders from multiple jurisdictions, the same was selected for the present discussion. The time involved in criminal prosecutions cannot be side-lined. Moreover, the new legislation does not clarify the procedure for initiating the criminal penalties. Therefore, we suggest having 'consumer-oriented' legislation instead of 'punishment-oriented' by entitling a heavy compensation to the consumers. For the consumers deceived by misleading advertisements, it is argued that the

criminal sanctions are an effective means as the advertisers' criminal intent is reflected in the deliberate and inaccurate representations.

Part 2 traced the origins of product liability from the contractual understanding out of the *Carlill* judgment and the strict liability theory as applied in the *Escola* judgment. It is argued that due to the dominating role of manufacturers in their relationship with a consumer, strict liability upon them strongly enforces consumer protection. However, some clarity is required in the liability of the intermediaries such as wholesalers and service providers as they also rely on the branding performed by the producers.

The emerging field of Artificial Intelligence has attracted significant research across borders. In Part 3, we analyzed that AI systems carry a significant potential to cause widespread damage with the help of the Robodebt scandal in Australia, and dug into the possibilities of imposing strict and criminal liability upon the AI systems and robots. It can be seen that both liabilities conveniently blame the producer of an AI machine, but remain unsuccessful in imposing the liability on the advanced systems. A similar line of approach is followed in the present consumer legislation. Therefore, in order to successfully address the question of imputing liability over AI systems, it is imperative to make amendments in the law to incorporate definitional clauses highlighting the inbuilt artificial mechanisms of a product.

BIG DATA TECHNOLOGY- A PARADOX TO CONTEMPORARY CONSUMER'S CONSENT IN THE GLOBAL MARKET

[*]Dhruthi C & [**]Hima M

ABSTRACT

The global market is known for its inclusion of the latest technologies and progression towards a better approach to consumers. With this shift in the market, the meaning of a 'consumer' has become sophisticated. It has also resulted in various fallacies and one such concern is the concept of Big Data with respect to the privacy of consumers. Irrespective of whether there is consumer's consent, corporate companies, governmental agencies and foreign organizations have access to their personal information. It can be evolved into valuable data, which is used for various purposes, other than using it for keeping a track for marketing purposes. A policy as such must be formulated which balances the functioning of the market and protects the rights of consumers. The paper throws light upon the necessity of a specific policy to deal with the modern problems and inclusion of technology in policy making. In a nutshell, an interdisciplinary approach is adopted to discuss the need to protect the interests of consumers in the present market conditions and dynamically changing attitudes.

I. BIG DATA- A CONTEMPORARY CHALLENGE

As our society grows more complex, interconnected, and technologically advanced, data is generated that reflects this societal change, and potentially allows us to better understand this complexity.[1] The whole process of data collection itself has become a pivotal target for companies and other institutions to increase their profits and scrutinize their businesses. Perhaps, the collection of data related to consumers is an outlook of business strategies in today's global market.

[*] Dhruthi C, 3rd year, BA. LLB, JSS Law College, Autonomous, Karnataka.
[**] Hima M, 3rd year, BA. LLB, JSS Law College, Autonomous, Karnataka.

[1] G. West, *Big Data Needs a Big Theory to Go with it*, SCI, available at https://www.scientificamerican.com/article/big-data-needs-big-theory/., last seen on 21/10/2020.

The above idea was conceptualized into a reality through the advent of Big Data technology. Big Data may involve personal data: that is, any information relating to an individual, and can be anything from a name, a photo, an e-mail address, bank details, posts on social networking websites, medical information, or a computer's IP address.[2]

The European Commission defines Big Data as: *"Large amounts of different types of data produced from various types of sources, such as people, machines or sensors. This data includes climate information, satellite imagery, digital pictures and videos, transition records or GPS signals."*[3]

Thus, with technology, every individual's movements, decisions, and purchases—every recordable detail of their lives—is captured and memorialized in the electronic realm. Due to the exponentially increasing efficiency of storage, the data is collected in centralized servers, stored, and analyzed in other ways that were never before possible.[4]

Data, in its raw form is obtained through numerous ways, which includes collection through websites, cookies, social media, company records and so on. Many a times, the consumers are either unaware or negligent, and end up providing information that is needed and expected by such institutions.

The age of information has resulted in complex issues for informational privacy. These issues arise from the nature of information itself. Information has three facets: it is not rivalrous, invisible and recombinant. Information is not rivalrous in the sense that there can be simultaneous users of the good – use of a piece of information by one person does not make it less available to another. Secondly, invasions of data-privacy are difficult to detect because they can be invisible. Information can be accessed, stored and disseminated without notice. Its ability to travel at the

---

[2] Director General for Justice and Consumers*, The EU Data Protection Reform and Big Data: Factsheet 2016*, Commission Europe, available at https://publications.europa.eu/en/publication-detail/-/publication/51fc3ba6-e601-11e7-9749-01aa75ed71a1, last seen on 21/10/2020.

[3] Ibid.

[4] C. Devins, T. Felin, S. Kauffman & R. Koppl*, The Law and Big Data*, 27 Cornell Journal of Law and Public Policy 357, 363 (2013), available at https://www.lawschool.cornell.edu/research/JLPP/upload/Devins-et-al-final.pdf, last seen on 12/11/2020.

speed of light enhances the invisibility of access to data, 'information collection can be the swiftest theft of all'. Thirdly, information is recombinant in the sense that data output can be used as an input to generate more data output.[5]

Thus, complex steps are involved in constituting Big Data owing to its volume, velocity, variety and value. The data collected shall be sorted and the important statistics shall be extracted (also known as data mining). Such valuable insights shall be stored for further analysis and extraction. The data analysis is the crucial phase, wherein such valuable information shall be further divided into many databases, each under different categories of studies associated with behavioral pattern, reasoning and approach towards market conditions and changes. Thus, what seems to be plain information for a layman, holds beneficial value for associated businessmen and other functionaries.

With the advent of the Internet of Things (**"IoT"**), more objects and devices are connected to the internet, gathering data on customer usage patterns and product performance. The emergence of Machine Learning (**"ML"**) has produced still more data. While Big Data has come far, its usefulness is only just beginning. Cloud computing has expanded Big Data possibilities even further. The cloud offers truly elastic scalability, where developers can simply spin up ad hoc clusters to test a subset of data.[6] The development and extensive use of highly distributed and scalable systems to process Big Data is widely considered. New data management architectures, e.g., distributed file systems and NoSQL databases, are used in this context.[7]

Thus, advancement in the field of Big Data is an ongoing process with the improvement in technology, science and research. Though it's a beneficial

[5] C.P. Moniodis, *Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy*, 15 (1) Yale Journal of Law and Technology, 139, 153 (2012), available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1080&context=yjolt, last seen on 20/10/2020.
[6] *The definition of Big Data*, Oracle, available at https://www.oracle.com/in/big-data/what-is-big-data.html#link4, last seen on 20/10/2020.
[7] J. Pokorný, K. Saeed & V. Snášel, *How to Store and Process Big Data: Are Today's Databases Sufficient?* International Federation for Information Processing, 5, 5 (2014), available at https://hal.inria.fr/hal-01405547/document, last seen 20/10/2020.

tool for global markets, it's hampering the rights of consumers. Big Data is rather a loop which has no end to it. Technology is the strongest weapon and data is the propellant to it. Since its difficult to trace the source or track the flow of data over the internet and other databases, misuse of it is bound to happen. Hence, with the improvement and dependence on Big Data, additional responsibilities have to be borne by the collector.

II. CHANNELS AND ULTERIOR EFFECTS OF BIG DATA VIS-À-VIS PRIVACY AND CONSENT

Big Data is an excellent tool which facilitates in pooling gigantic amount of information. Any technology in itself does not provide for a diversion from its purpose, rather myriad channels are adopted by people using such a kind of technology for their personal gains and losses.

Privacy for a person is the space which must be ultimately untouched, but is also the most abused right. Once the personal data is collected, it is shared and reshared, sold and re-sold to an extent that it no longer remains 'personal' and 'private'.

Data brokers are companies that aggregate information about consumers from different sources, then license or sell that information to other organizations.[8] Data brokers hoover up personal identifiable information – in which specific information distinguishers can be traced or attributed to an individual's identity. The more data obtained, the more granular a profile of an individual can be.[9]

To begin with, by buying or licensing data or scraping public records, third-party data companies can assemble thousands of attributes each, for billions of people. For decades, companies could buy up lists of magazines subscribers to build targeted advertising audiences.[10] The information most

[8] M. Wlosik, *What is a Data Broker and how does it work?,* Clear Code, available at https://clearcode.cc/blog/what-is-data-broker/#what-are-data-brokers?, last seen on 12/12/2020.

[9] D. Leong & T. Yi-Ling, *Data Brokers: A Weak Link in National Security*, The Diplomat (21/08/2020), available at https://thediplomat.com/2020/08/data-brokers-a-weak-link-in-national-security/, last seen on 24/10/2020.

[10] S. Melendez & A. Pasternack, *Here are the data brokers quietly buying and selling your personal information*, Fast Company, available at https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information, last seen on 24/10/2020.

closely related to one's spending habits is usually the most valuable to data brokers. Some of the data businesses are looking for, and can easily obtain information on household income, size and the ages of the members of your family, investment propensity, frequency by which you make large purchases, age and gender, educational status, general interests, and how you tend to spend your money on, like major life changes such as marriage, the birth of a baby, or retirement.[11] These profiles are then licensed or sold to companies to inform their business operations in marketing or in advertising products and services to customers. Companies utilize data-driven marketing to deliver more targeted and profiled advertising to consumers.[12]

Third party threats are a growing concerning too. Banks should also make sure they are only working with third parties that have appropriate security infrastructure in place, to mitigate the chance of any data being stolen.[13] It is important to gain access to third party environments or applications that can access the primary parties' database.

Apart from this, data tracking is another concern. Once the data of consumers is collected, the data analysts work towards analyzing that piece of information and try to reproduce as many pieces of information as possible. For the process to continue, they track all of our online behavior, with the available information. Thus, a simple mechanism with complex procedures to track the market behavior of consumers, opens a door for another business.

Seeing from the perspective of business, this seems a threat to the birth right of every individual. But from a wider perspective, such personal information of individuals can be a threat to the nation's security too. Data protection has become an important objective of countries around the globe. The need to keep a tab on data flow is necessary. Since such data

[11] *What is Big Data analytics and what does it mean to the consumers?,* Money Crashers, available at https://www.moneycrashers.com/big-data-analytics-consumers/, last seen on 24/10/2020.
[12] Supra 6.
[13] K. Flinders, *Digital bank customer data breached through third party*, Computer Weekly (28/07/2020), available at https://www.computerweekly.com/news/252486767/Digital-bank-customer-data-breached-through-third-party, last seen on 25/10/2020.

obtained is exploited commercially in the later stages, the ultimate source to obtain it is unknown.

Most legacy systems can't cope with the growing workload. Trying to collect, store, and analyze the required amounts of data using an outdated infrastructure can put the stability of your entire system at risk. With so many different kinds of data and its total volume, it's no surprise that businesses struggle to cope with it. This becomes even more obvious when trying to separate the valuable data from the useless.[14]

Such data can be accessed by anybody. Some countries are trying to ensure that the geolocation information is stored locally for national security considerations since having access to important information internationally can make a difference in a conflict. But companies in countries with rigid data residency and access requirements will acquire less crucial information in times of emergency because they are not trusted by business partners and governments abroad. Some countries seem to believe that crucial information will be safer at home. But, countries with isolated or outdated technology are less able to protect locally stored data against foreign military and criminal threats.[15] One of the chief concerns which the formulation of a data protection regime has to take into account is that while the web is a source of lawful activity-both personal and commercial, concerns of national security intervene since the seamless structure of the web can be exploited by terrorists to wreak havoc and destruction on civilized societies.[16] The modern warfare would happen not with weapons and missiles, but with this data, while sitting behind the computer.

Apart from diversion of right to privacy, Big Data can become a personal threat to the consumer himself and can expose him to various cybercrimes. Big Data companies like Amazon heavily rely on distributed computing, which typically involves data centers geographically dispersed across the

[14] A. Chalimov, *Big Data in the banking industry: the main challenges and use cases*, Eastern Peak (10/01/2019), available at https://easternpeak.com/blog/big-data-in-the-banking-industry-the-main-challenges-and-use-cases/, last seen on 25/10/2020.
[15] *How data residency laws can harm privacy, commerce and innovation - and do little for national security*, World Economic Forum (09/06/2020), available at https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/, last seen on 25/10/2020.
[16] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

whole world. Amazon divides its global operations into twelve regions each containing multiple data centers and being potentially subject to both physical attacks and persistent cyberattacks against the tens of thousands of individual servers housed inside.[17]

The consumer might have consented to the terms and conditions, but whether it is a consent to put their data on sale is the question. An informed consent, in present situation is not 'informed' *prima facie*. Definitely, the consumers would not have consented for the above ulterior effects through Big Data analytics. Consent, should be expressed restrictively in a sensitive matter, rather than assuming the broadest interpretation. Informed Consent must be prevented from being misused as a defense by the market.

As big is the Big Data, so are its consequences. If the size of the data is big enough, precise personal information can be obtained. A healthy market system must be a one, which benefits itself with the benefit of all. At the same time, such a system cannot be maintained as it operates in an *in vivo* environment and is susceptible to changes, fashions and attitudes of humans. But such susceptibility must not expose the consumer, the main component of this system, to face adverse consequences. A relation of harmony and trust must be established in every operation of business. Profits and other gains must not cost an individual's privacy.

III. 'CONSUMER' - THE DYNAMICALLY CHANGING STATUS UNDER PRIVATE FUNCTIONARIES

The meaning of consumer must be analyzed considering the fact that the market too has changed its way of business. Plainly, a consumer is a person who buys goods and services in exchange for consideration. But the process of buying itself has become advanced and complex, with the advent of technology. E-commerce has opened the gate for the market to move faster. Diversity is an attributed factor to it.

[17] J. Ryoo, *Big data security problems threaten consumers' privacy*, The Conversation (23/03/2016), available at https://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798, last seen on 25/10/2020.

Institutions which analyze electronic data can build a user's behavior profile which contains attributes like the user's browsing history, transaction history, sex, profession, earnings, age and other demographics. The user behavior profile can be used to provide a more accurate and specialized service.[18] In such as system, the concept of consumerism is no longer archaic. Thus, it is essential to clarify the status and meaning of a consumer with respect to various institutions, impact of Big Data on them and misuse of consent.

1. Electronic Banking or E- banking

A customer is the one who uses a financial institution's services for their benefit. Significant progression in Information Technology has created a universal revolution in financial institutions. Substantial changes in financial systems are initiated by globalization and financial liberalization.[19]

Big Data analytics is now being implemented across various spheres of banking sector, and is helping them deliver better services to their customers, both internal and external, along with also helping them improve on their active and passive security systems. Banks today use spending patterns of their customers, perform consumer behavior based analysis on their channel usage, consumption patterns and segment consumers, to identify potential customers for selling financial products.[20] By integrating and analyzing data, banks have an opportunity to get a more accurate view on their customer's preferences.[21] The latest progress in

---

[18] S. Sharma, *A study on data mining horizons*, 2 International Journal of Recent Trends in Engineering & Research, 322, 322 (2016), available at https://www.ijrter.com/papers/volume-2/issue-4/a-study-on-data-mining-horizons.pdf, last seen on 26/10/2020.

[19] R.A. Aziz, R.E. Badrawy & M.I. Hussien, *ATM, internet banking and mobile banking services in a digital environment: The Egyptian banking industry*, 90 International Journal of Computer Applications, 45, 45 (2014), available at https://www.researchgate.net/publication/327534978_ATM_Internet_Banking_and_Mobile_Banking_Services_in_a_Digital_Environment_The_Egyptian_Banking_Industry, last seen on 26/10/2020.

[20] U. Srivastava & S. Gopalkrishnan, *Impact of Big Data Analytics on Banking Sector: Learning for Indian Banks*, Science Direct, available at https://www.sciencedirect.com/science/article/pii/S1877050915005992#:~:text=Banks%20reap%20the%20most%20benefits,for%20themselves%20and%20their%20customers.&text=Customer%20Segmentation%20and%20Profiling,profiling%20to%20increase%20hit%20rate, last seen on 27/10/2020.

[21] N. Sun, J.G. Morris, J. Xu, X. Zhu & M. Xie, *iCARE: A framework for big data-based banking customer analytics*, 58 International Business Machines Corporation Journal,

Information Technology makes it possible to integrate and analyze millions of records which include personal data.[22]

Increased competition and fast paced technological innovation in financial markets have forced banks to invest in online banking systems and other financial delivery channels to retain competitive advantage, revitalize customer relationship management and give customers the opportunity to perform real time financial actions easily and independent of time and place.[23] Perceived risk is one of the main inhibitors for internet banking usage and can be described as a customer's opinion of uncertainty and probable negative consequences of making use of internet banking.[24] United States digital bank Dave has reported a breach of customer data after hackers gained access through third-party technology supplier.[25] Passwords, as well as personal user information such as names, e-mails, birth dates, addresses and phone numbers, were included.[26]

In order to keep up the pace, E-banking websites often fail to protect the obtained data of consumers. Neither the consumer's consent is taken while pooling their data nor it is duly protected. Most of the activities occur through online transaction. Consumers are bound to update their bank details and other personal information to do so. Thus, such data is susceptible to be mined by the institution itself. Such Big Data pool is also

---

Research and Development, 1, 1 (2014), available at https://www.semanticscholar.org/paper/iCARE%3A-A-framework-for-big-data-based-banking-Sun-Morris/8e48fdca32b7b5bcb74cc5b3e6a2585b544c7cea, last seen on 27/10/2020.

[22] S.T. Ahmad, S. Haque & S.M.F. Tauhid*, A details study of data transformation for privacy preserving in data mining*, 5 International Journal of Scientific & Engineering Research, I, 2 (2014), available at https://www.ijser.org/paper/A-Details-Study-of-Data-Transformation-for-Privacy-Preserving.html, last seen on 28/10/2020.

[23] A.A. Shaikh & H. Karjaluoto, *Mobile banking services continuous usage-Case study of Finland*, 1 International Conference on System Sciences, 1497, 1497 (2016), available at https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNB7cjja/pdf, last seen on 28/10/2020.

[24] J.R.S. Fonseca, *E-banking culture: A comparison of EU 27 countries and Portuguese case in the EU 27 retail banking context*, 21 Journal of Retailing and Consumer Services, 708, 709 (2014), available at https://www.sciencedirect.com/science/article/abs/pii/S096969891400068X, last seen on 28/10/2020.

[25] A. Hrushka, *Dave security breach exposes 7.5M users' data,* Banking Drive (28/07/2020), available at https://www.bankingdive.com/news/dave-security-breach/582426/#:~:text=A%20security%20breach%20exposed%20the,Waydev%20was%20breached%2C%20Dave%20said, last seen on 12/12/2020.

[26] Supra 13.

exposed to various dangers, including hacking. The data sold thereupon exposes the consumers to cyber identity thefts, phishing, credit and debit card frauds and so on.

2. E- Education Facilities

Since education is a service and students enjoy it by paying at least minimal fees in extremities, they are the consumers. Educational Institutions are covered by the provisions of the Consumer Protection Act, 1986 ("**CPA, 1986"**).[27] If a student is aggrieved by the service/if an educational institution's service has a deficiency, a student can avail justice. Education sector has been streamlined to compete in the market. Various online education services are blooming rapidly. Students have access to online courses and distance education courses, provided online by various educational institutions. Though the service is delivered through many ways, the service intended to be delivered remains the same. Thus, such online service providers use the cyber platform to dispense their services, and students provide their information along with other data during enrolment and registration process.

In many cases, while in college, students begin to prepare themselves, financially, for the rest of their lives. They apply for jobs, rent apartments, and purchase vehicles. Such endeavors require financial stability, therefore, having personal data stolen could be detrimental. Larger universities hold more faculty, student and alumni data, proving that the more records a university holds, the more likely they are to be breached.[28] Schools face high costs as a result of data breaches. A study by the Ponemon Institute shows that the average cost of a data breach is USD 141 per record, but in education it typically reaches USD 200 per record (and has been even higher, with the four-year price averaging USD 260).[29]

---

[27] The Consumer Protection Act, 1986.

[28] M. Samantha, *Data Breaches in Higher Education Institutions,* University of New Hampshire Scholar Repository*,* available at https://scholars.unh.edu/honors/400, last seen on 27/10/2020.

[29] R. Carr, *The Rise of Education Data Breaches*, Zettaset, available at https://www.zettaset.com/blog/education-data-breaches/, last seen on 27/10/2020.

Big Data can impact higher education practices, from attractive student experiences to improved academic programming, to more effective evidence-based decision making, and to strategic response to changing global trends, but has the potential to turn complex, often unstructured data into tortious information.[30] In addition, monetary variables such as high-income students, faculty salary, and median and average family income show significance. The more data elements a university protects, the less likely a breach will occur. This indicates that universities should not only be taking actions to secure privacy but also to ensure the most amount of data possible is suppressed.[31]

Online education start-up Edureka suffered a significant data leak that exposed sensitive personal information such as names, addresses, phone numbers of at least 2 million users. *"Given that Edureka provides professional-grade online courses to people, often in significant or powerful positions and with access to highly-sensitive information, the company's compromised server security could have been devastating to entire organizations such as universities, companies or government departments"* said a lead security researcher of that case.[32]

Escola Digital, a Brazil-based online learning platform, suffered a data leak that exposed over 75,000 private records (15MB) of students and teachers.[33] South Africa-based online learning platform MyTopDog lost over 800,000 students' personal records (40-50MB).[34] Okoo, a Kazakhstan-based online course portal, lost around 7,200 records (418MB) that held students' personally identifiable information and administrative data.[35] The U.S.-based online education platform Square Panda lost around 15,000 personal records (1MB) of parents and teachers.[36] S.-based virtual learning

[30] M. Hilbert, *Big Data for Development: From Information- to Knowledge Societies*, SSRN, available at http://ssrn.com/abstract=2205145, last seen on 27/10/2020.
[31] Supra 23.
[32] Salman SH, *Edureka's database breached, 2 million user records potentially at risk,* LiveMint, available at (30/09/2020) https://www.livemint.com/companies/start-ups/edureka-s-database-breached-2-million-user-records-potentially-at-risk-11601450797202.html, last seen on 27/10/2020.
[33] C. Williams, *Data leaks in Online education: Almost 1 million data exposed,* WizCase (02/10/2020), available at https://www.wizcase.com/blog/educational-breaches-research/, last seen on 16/12/2020.
[34] Ibid.
[35] Ibid.
[36] Ibid.

platform Playground Sessions' data leak exposed nearly 4,100 user records (1.2MB).[37]

Presently, most of the universities are not equipped with a strong and protected system to protect such data. Considering the other institutions, mining data from websites and other databases of educational institutions is an easier option. Generally, such websites give public access for viewing the functioning of the institutions, their alumni profile, portfolio of the teaching faculty and so on. Anyone can easily access data through this means. Institutions provide student grant facilities, wherein data regarding their profile and other information shall be stored. If leaked, it can be used for many ulterior motives, or even sold to companies by data brokers and hackers. Consent of students for such dangers is a silent factor.

3. Medical Institutions and Tele-Medication

Telemedicine is a modern and a scientific approach in health care system with the use of telecommunication and information technologies to provide clinical health care at a distance. Telemedicine also referred to as telehealth allows health care professionals to evaluate, diagnose and treat patients in remote locations using telecommunication.[38] Telenursing is defined as the use of telecommunication technology to deliver nursing services to client at a distance.[39] Nurses engaged in telenursing practice continue to assess, plan, intervene, and evaluate the outcomes of nursing care, but they do so using technologies such as the internet, computers, telephones, digital assessment tools, and telemonitoring equipment.[40] Bearing in mind that health services now provided via tele-technologies

[37] *E-Learning Platforms Continue to Suffer Data Breaches; 1 Mn Records Exposed*, Cisomag (20/07/2020), available at https://cisomag.eccouncil.org/data-breaches-on-e-learning-platforms/, last seen on 27/10/2020.

[38] S.K. Passyavula, *Telemedicine, telenursing & tele education -A revolution multi-innovation in current nursing scenario*, 2(5) International Journal of Medical and Health Research, 31, 32 (2016), available at http://www.medicalsciencejournal.com/archives/2016/vol2/issue5/2-5-23, last seen 28/10/2020.

[39] J. J. Fitzpatrick & M. Kazer, *Encylopedia of Nursing Research*, (3rd ed., 2011).

[40] Peck, Amy RN, *Changing the Face of Standard Nursing Practice Through Telehealth and Telenursing,* 29(4), Nurse Administration Quarterly, 339, 340 (2005), available at https://journals.lww.com/naqjournal/Citation/2005/10000/Changing_the_Face_of_Standard_Nursing_Practice.8.aspx, last seen on 16/12/2020.

have expanded, the term telehealth is used to capture the breadth of services.[41]

A patient is a consumer since he enjoys the service of the doctors and medical fraternity for the fees paid. Though health care is removed from the meaning of service under Section 2(42) of the Consumer Protection Act, 2019 (**"CPA"**),[42] it contains the phrase "*includes, but not limited to"* and the same is an inclusive clause. It directly points out to the fact that 'healthcare' can still be included and interpreted under Section 2(42) of the CPA.[43] Since this is discharged via online nowadays, concerns regarding privacy policy and data mining come into issue. Thus, a patient is still a consumer and implied consent of his to enjoy services online should not be mistaken as a nod to compromise with privacy.

The personal data of 2,373,764 patients was left exposed online after Hova Health, a telemedicine company based in Mexico, misconfigured a MongoDB database. The database contained patient names, personal ID codes for Mexican citizens and residents, insurance policy numbers and expiration dates, dates of birth, and addresses. There also were flags noting migrant status or disabilities.[44] Misconfiguration issues are far too common for the healthcare sector, which already is being pummeled by cyberattacks. One wrong click and tens of thousands to millions of patient records can be breached.[45] Telehealth start-up Babylon Health just suffered a data breach that mistakenly sent videos of patients' private consultations with

---

[41] L. Schlachta-Fairchild, V. Elfrink & A. Deickman, *Patient Safety, Telenursing, and Telehealth*., In. Patient Safety and Quality: An Evidence-Based Handbook for Nurses, (Hughes RG, Rockville (MD): Agency for Healthcare Research and Quality (US); 2008 Apr. Chapter 4). available at https://www.ncbi.nlm.nih.gov/books/NBK2687/, last seen on 28/10/2020.

[42] The Consumer Protection Act, 2019.

[43] S. Paliwal & G.S. Gaur , *Exclusion Of 'Healthcare' From The Definition Of 'Service': A Delusional Relief For Medical Professionals*, Mondaq (11/08/2020), available at https://www.mondaq.com/india/healthcare/975294/exclusion-of-healthcare39-from-the-definition-of-service39-a-delusional-relief-for-medical-professionals, last seen on 28/10/2020.

[44] J. Davis, *Telemedicine vendor breaches the data of 2.4 million patients in Mexico*, Healthcare IT News (07/08/2018), available at https://www.healthcareitnews.com/news/telemedicine-vendor-breaches-data-24-million-patients-mexico, last seen on 02/11/2020.

[45] Ibid.

doctors to other patients.[46] The breach was brought to Babylon Health's attention after a patient tweeted a screenshot, showing he had access to dozens of other people's consultation videos.[47] As the numbers of new and innovative technologies emerge, researchers and developers must remember the security of patient information, regardless of how it is transmitted.[48]

4. E- Commerce

Modern consumer's activity of shopping necessities and luxuries have been operated online increasingly. With discounts and gift vouchers available throughout the year, consumer's first choice is online shopping, through E- commerce websites.

The *modus operandi* is that a consumer has to create an account, view and order a product and choose one among various payment methods. Most of the time, consumers pay online via various payment methods. Phone numbers and E-Mail IDs are collected. Thus, such platforms keep a track on category of items a consumer constantly views and sends messages regarding current deals. This proves that e-commerce websites keep track of our information and preferences via Big Data technology. But ensuring the safety of such information is necessary. As the consumers are reaping benefits from online services as such, they are getting exposed to numerous cyber threats, where personal data is sold for a price.

User data from online grocery platform BigBasket is for sale in an online cybercrime market. The data comprised names, E-Mail IDs, password hashes, PINs, mobile numbers, addresses, dates of birth, locations, and IP addresses. Part of a database containing the personal information of

[46] L. Kelion, *Babylon App admits GP app suffered a data breach,* BBC News (09/06/2020), available at https://www.bbc.com/news/technology-52986629, last seen on 16/12/2020.
[47] A. Holmes, *A telemedicine app accidentally leaked videos of people's medical consultations to other patients*, Business Insider (10/06/2020), available at https://www.businessinsider.in/tech/news/a-telemedicine-app-accidentally-leaked-videos-of-peoples-medical-consultations-to-other-patients/articleshow/76307541.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, last seen on 02/11/2020.
[48] Supra 20.

close to 20 million users was available with a price tag of INR 3 million (USD 40,000).[49]

Thus, one point to conclude from the above information is that the consumers are not the main facet, but a part and parcel of the global profit system. A consumer's consent should be taken, and such consent shall not be implied as a green signal to use his rights and personal space as a raw material. When a website requests for personal information, it is a bounden duty to protect it.

IV. E-GOVERNANCE, BIG DATA, CONSUMER CONSENT AND PRIVACY

Governments in any given country will have a wide-ranging purpose for amassing data, which reflects to be differing from that of businesses to a considerable extent. The key intention of businesses to collect data is to achieve profits and keep the customers happy and satisfied. But the distinctive object of the government includes maintaining domestic peace and tranquility, achieve sustainable development, secure citizen's basic rights, promote general welfare and economic growth.[50] In all, the

[49] S. Gosh, *Apparent data breach at BigBasket reveals the need for e-commerce players to bolster cybersecurity measures*, CSO India, available at https://www.csoonline.com/article/3596873/apparent-data-breach-at-bigbasket-reveals-the-need-for-e-commerce-players-to-bolster-cybersecurity.html, last seen at 10/01/2021; *BIGBASKET, India's leading online supermarket shopping allegedly breached personal details of over 20 million people sold in Dark web*, available at https://cybleinc.com/2020/11/07/bigbasket-indias-leading-online-supermarket-shopping-allegedly-breached-personal-details-of-over-20-million-people-sold-in-darkweb/?__cf_chl_captcha_tk__=5711add3a5e2c69e10165212b8435433b0a5dfce-1610302048-0-ARSairp5Z40FiaO_3gb_UYsO7Izw6xBYq7ASBXimg5-kpJ126nWEUXA_xje9_uykMuX-Cx3o6nHqSrj52IUar4Lr3Blo0NBgv-Kj_w8Fe0MYw3Z4KiYgFfjzdV2aptwBGZrSuErqjB54Fo3urMj9hh2lpB9TjZEN1ZgRR2tdSp1P3CWLt7oGP3XwD0YFsq9jhshbNkpeDZ2NHXVTflDcTAaB-F8wRk2DELowyP39RzK3VwyvJPTPLFD2e9hLtXj978Wm5fEL0CDR6lIJ8h2q-syu4flN6phetgGb7wNhV0CLXQnPTgjkyOzzLQHS8JFTlIZPnDHxYeeAyomMyXXJw0EO6YlO_BDVTX01yQlPIuEg7X6nPq0m0yTKeYsH_rtiUi_rirviO1CGvOHkhX-DTglErxP9J_7WMpSaVDNCHTwXo4ZUqTuv59ZXwlNHadD6Y-qXifdm8GC2FdM0Nm21fxrsHwjJxEZp1-uIKCDlqMh9Mk6UkFliqJH6nIBpe9FDdP8jYAPslvuMWePkYk2o0aQMRI8i5nHIwyQrkOrZJhICxFxb-G7z2EWJZw5tf3grM9NXxP4M62mcFIaXrwQXcrnoTrUrV4qZHWMVem7huK_hPbkGk5u6nW3MZ0J0VD_7b6FwGV7zxCG-HuDbFazko64UptU49LeUnwV--gxVoqiP_uxhLetjSvaX5xiJQeN7BWwuHcr5SQXPj_OpM9z-S6o, last seen on 10/01/2021.

[50] G. Kim, S. Trimi & J. Chung, *Big-Data Applications in the Government Sector*, Communications of the ACM, March 2014, Vol. 57 No. 3, Pages 78-85, available at https://cacm.acm.org/magazines/2014/3/172509-big-data-applications-in-the-government-sector/fulltext#R18, last seen on 02/11/2020.

government's target revolves around the citizens and their well-being. These targets are achieved by rendering services to the citizens by different government departments. The conventional mode of performing these functions is through offline mode wherein the citizens visit respective offices where the desired services are rendered.

A significant dilemma of whether government services can be held liable for deficiency of service under the CPA, 1986 has been elucidated in various cases like *Shamsher Khan* v. *Rajasthan State Electricity Board*[51] where the applicant had applied to Electricity Board for electricity connection for a flour mill but there was a delay in releasing the connection. He filed a complaint for deficiency in service and was held a consumer under the Act. Thus, a statutory corporation which is a government body was held liable for deficiency in service.

Similarly, in *Shri Prabhakar Vyankoba Aadone* v. *Superintendent, Civil Court*[52] ***("Aadone")***, the National Commission held that an applicant for certified copy of a judicial order, who deposits a fee for obtaining such copy is a 'Consumer' within the meaning of the CPA, 1986 and the processing of such application and the preparation and delivery of the copy in consideration of the copying charges/fee by the concerned staff attached to the court would be a service within the meaning of the Act. This view was further upheld by the Commission in *Dr. Chandrakant Vitthal Sawant* v. *L. R. Pilankar Inspector of Land Records*[53] ***("Vitthal")***, in which it was held that the petitioner who had approached the respondent authority for carrying the measurement of the land in question by paying the requisite fees is a consumer and the functions of the respondent would constitute service.

E-Governance or electronic governance can be defined as the application of information and communication technology (**"ICT"**) for providing government services, exchange of information, transactions, integration of previously existing services and information portals[54]. The perspective of

[51] Shamsher Khan v. Rajasthan State Electricity Board, (1993) II CPR 6 (Raj.).
[52] Shri Prabhakar Vyankoba Aadone v. Superintendent, Civil Court, 1986 2004 Consumer 7211 (NS).
[53] Dr. Chandrakant Vitthal Sawant v. L. R. Pilankar Inspector of Land Records, 2013 SCC Online NCDRC 642
[54] F. Barrister & R. Conolly, *Defining e-Governance*, e-Service Journal 3, 4 (2012).

e-governance is *"the use of the technologies that both help to govern and have to be governed"*.[55] The central goal of e-governance is to reach the beneficiary and to ensure that their service needs are met. With the surge to associate digitalization with the ideology of welfare state, the need for e-governance transpired. Every Ministry, government departments, agencies could now function, store and update records, attend to the needs of the citizens through their websites or mobile applications.

Through Section 2(7) of the CPA the government widened the definition of 'consumer' by inserting explanation (b) which states that, the expressions 'buys any goods' and 'hires or avails any services' includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing.[56] The central government has been allowed to take steps and draft guidelines to discourage discriminatory e-commerce activities in order to protect customers' privileges and interests. The CPA, 1986 did not specifically include e-commerce transactions, and this lacuna has been addressed by the new Act. Now, a new dilemma arises: whether the citizens availing the services of e-governance are 'consumers' and whether services provided through e-governance constitute 'service' under the CPA. And if it does, will the government be liable for misuse of personal data or violation of privacy of the citizens stored in the Big Data bank.

In its website, the Ministry of Consumer Affairs has included e-governance division where it declares its vision: *"Make all Government services accessible to the common man in his locality, through common service delivery outlets, and ensure efficiency, transparency, and reliability of such services at affordable costs to realize the basic needs of the common man"*[57]

It further declares: *"The Government of India is focused on using technology to the maximum possible extent to give fillip to effective and efficient governance. To achieve the objective of providing consumer-friendly services, the department has digitized its various*

[55] P. Rossel & M. Finger*, Conceptualizing e-Governance Management* (2007): 399–407.
[56] Explanation (b), S. 2(7), The Consumer Protection Act, 2019.
[57] Department of Consumer Affairs, *E-governance,* Ministry of Consumer Affairs, Food and Public Distribution, available at https://consumeraffairs.nic.in/organisation-and-units/division/e-governance, last seen on 08/11/2020.

functions." Thus, relying on the declaration, services provided through e-governance to the citizens makes them consumers.

The goal of government-to-citizen (**"G2C"**) e-governance is to offer a variety of ICT services to citizens in an efficient and economical manner and to strengthen the relationship between government and citizens using technology.[58] Mundane services such as name or address changes, applying for services or grants, or transferring existing services are more convenient and no longer have to be done in person.[59]

The citizens avail these e-services through the respective department's website/portal by paying the prescribed fee. As held in *Aadone* and *Vitthal,* the charges paid while applying for the services is consideration fee and the function of the office constitutes service. Thus, a consumer and service provider relationship are established between the citizen and the government when consideration fee is paid for the service.

Through e-governance platforms, the government is functioning at an improved efficiency, reliability and pace. With this development, the gravity of application of Big Data was realized. Until the recent years, utilization of Big Data by the government was spotted only for keeping tabs of huge data produced in the course of functioning of various governmental ministries, departments, agencies, intelligence services, etc. But with the foundation of e-governance, the velocity at which data is produced is enormous. Technology relating to Big Data is developed to an extent where a humungous amount of data produced like in the Unique Identity Project, Digital India program, etc. can be collected, stored and analyzed for any desired outcome.

With the view to provide value-added services to citizens through e-governance, the government has failed to address the shortcomings of digitalization on the privacy of citizens. In fact, the privacy issues dominate over the benefits of e-governance in every digital platform that the government has introduced.

---

[58] *E- governance*, Wikipedia, available at https://en.wikipedia.org/wiki/E-governance, last seen on 16/12/2020.

[59] W. Miller & J. Walling, (2013), *Government in the twenty-first century: New Avenues of Study*, *Taking Sides*. New York, NY: McGraw Hill.

One such case, is of Aadhaar, which is the world's largest biometric identity platform. With an enrolment of over 1 billion registrants,[60] Aadhaar exhibits data challenges like data volume, variety and velocity which are the characteristics of Big Data. This digital identity system facilitates both the government and private sector, the precious enormous data of residents. It has become the *de-facto* identity document accepted by all service providers like private banks, schools, hospitals, telecom operators to buy SIM cards, medical insurance or any other utility services. While availing any government service, citizens are required to provide their Aadhaar number which gets uploaded in their records and further on Big Data bank. The biometric identifiers which are considered to be a boon can pose a threat of data breaches and misuse of personal data which may lead to violation of privacy and human rights of the citizens.

Linking of Aadhaar to various accounts and documents like bank account, Permanent Account Number (**"PAN"**) card, social security schemes, mobile SIM cards, pension account, Liquefied Petroleum Gas (**"LPG**") connection, driving license possessed by the citizens has been made mandatory. Once linked with Aadhaar, all the data connected with these accounts and documents get stored in the Big Data bank. Any alteration made to them will get updated in the Big Data storage. Every document and account possessed by the citizens contain sensitive information of their lives, religion, sexual orientation, residential address, etc. Big Data technologies can potentially be used to discriminate against vulnerable groups and manipulate information. Following are the features of Unique Identity Project, Aadhaar which compromises the privacy of the citizens when the documents are linked:

1. The Central Identities Data Repository

Aadhaar database containing all Aadhaar numbers, demographic and biometric information is stored in Central Identities Data Repository

[60] *AADHAAR Dashboard*, Unique Identification Authority of India, available at https://uidai.gov.in/aadhaar_dashboard/index.php, last seen on 16/12/2020.

(**"CIDR"**) which is a centralized database.[61] Both username (Aadhaar number) and the password (biometric information) being stored in this same database has made the citizens' personal data vulnerable to misuse. Further, the Aadhaar database is stored in about 7000 servers in two data centers located at Bangalore, Karnataka and Manesar, Haryana.[62] If any of the two data centers is compromised, there is no certain answer as to the consequence on the highly sensitive and personal data of millions of residents.

2. Ginger Platform

Service providers that adopt the Aadhaar number of the residents in their service delivery database i.e., seeding, will have to move their existing databases onto the Ginger platform, which then organizes the present and incoming data in the database by individual Aadhaar numbers. Once organized, anyone having access to the 'control' end of the Ginger platform can access all data associated to an Aadhaar number.[63] It further facilitates profiling of individuals through convergence of databases on this platform which can then be accessed by the Unique Identification Authority of India (**"UIDAI"**). The seeded data of the individuals containing inherent psychological and behavioral characteristics can be utilized by the Government or anyone with the access. Thus, the ginger platform lacks protection on the personal and sensitive information of the citizens.

3. Freedom of Speech and Expression

Every citizen's data will be collected and stored by different agencies throughout his lifecycle. The data begins from birth certificate, education, scholarships, driver's license, passport, employment, taxes, marriage

---

[61] Amber Sinha, *The Unique Identity Project, Big Data in Governance in India: Case Studies, The Centre for Internet and Society, India*, available at https://cis-india.org/internet-governance/files/big-data-compilation.pdf, last seen on 16/12/2020.

[62] *Aadhaar-enabled DBT savings estimated over Rs 90,000 crore*, The Times of India (11/07/2018), available at https://timesofindia.indiatimes.com/business/india-business/aadhaar-enabled-dbt-savings-estimated-over-rs-90000-crore/articleshow/64949162.cms, last seen on 05/11/2020.

[63] E. Hickok, S. Chattapadhyay & S. Abraham, *Big Data in Governance in India: Case Studies,* The Centre for Internet and Society, India, available at https://cis-india.org/internet-governance/files/big-data-compilation.pdf, last seen on 08/11/2020.

certificate, banking, insurance, land records, court records, pension to the death certificate. It is an individual's cradle to grave profiling which enables greater surveillance and impedes anonymity. This will have an adverse impact on a citizen's freedom of speech and expression.

Since there is no detailed privacy framework, therefore there are possibilities that the Authority may use Aadhaar Card data against citizens. For example, during a protest, law enforcement agencies can record the videos of protesters, scan the iris data, and easily access information about protesters. Access to sensitive data of this nature gives unfair advantage to repressive governments and protesters are vulnerable to threats.[64]

4. Data Protection Regulation

The government agencies and third parties, in the absence of specific data protection regulation and privacy legislations, can access and share data among them. A consumers' life can be made miserable at every step when data can be shared with secondary motives. Absence of specific regulation hinders human rights and freedoms of the consumers, while the technology sees new developments. With an aim to introduce a specific regulation, the Personal Data Protection Bill, 2019 (**"PDP"**) was drafted to protect the personal data of the individuals and prevent any form of misuse. But with provisions which empowers the government to collect and access personal data,[65] the Bill defeats its own purpose of safeguarding the privacy of the citizens.

Citizens while availing services from the government through offline or online mode become consumers and provide their utmost sensitive personal data to the government departments. Any breach of data and violation of citizens' privacy is equal to violation of rights and interests of the consumers.

[64] B. Halder, *Privacy in India in the age of Big Data*, APC, available at https://www.apc.org/sites/default/files/Privacy-in-India-in-the-Age-of-Big-Data.pdf, last seen on 09/11/2020.
[65] S. 98, Personal Data Protection Bill, 2019 (pending).

V. CURRENT LEGISLATIVE ACTIONS AND JUDICIAL OPINION ON BIG DATA

Big Data's advent in India markets and its influence on administration can be seen a decade later, compared to other developed countries. When other countries have backed up with a series of streamlined policies and regulations, India is still on its way to pass an effective, holistic and inclusive policy. The concept of Big Data and the importance of protecting information privacy was discussed for the first in *K. Puttaswamy* v. *Union of India.*[66]

The judgement vividly explained concerns regarding the nature of Big Data, i.e., these data sets are capable of being searched, they have linkages with other data sets, and are marked by their exhaustive scope and the permanency of collection. Also, it rightly opined that the challenge which is posed by Big Data mainly arises from State and non-State entities.

Emphasis was laid on the fact that the balance between data regulation and individual privacy raises complex issues requiring delicate balances to be drawn between the legitimate concerns of the State on one hand and individual interest in the protection of privacy on the other. Reference was made to the European data protection regime on the centrality of consent. It was held that a mere consent from the users is not a validation to exploit the data obtained and reuse it. The judgement also laid down that formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State.

With digital and technological revolution, India has welcomed multiple players into its market without establishing a formal regulation on data protection. Data revolution has reached to an extent where data mining has no legitimate boundary. The absence of specific regulation adds onto the inaccurate manipulation of data sharing, side-lining the most valuable aspect of the consumers i.e., privacy.

[66] Supra 16.

1. Information Technology (Amendment) Act, 2008

Certain aspects of data protection are covered under the Information Technology Act of 2000 (**"IT Act"**) and the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules of 2011 (**"Data Protection Rules"**). But the scope of these statutes is diminishing with enhanced technological developments.

The rules limit itself to companies, including firms, sole proprietorships, and associations of individuals engaged in commercial/professional activities (collectively, the 'body corporate')[67] and does not include government bodies and individuals engaged in data processing. This has contributed to validation of mass surveillance, profiling of individuals and misuse of citizen's personal data by the government which has an exponential impact on the individual's independence. Section 43A, which requires the *maintenance of reasonable security practices and procedures by bodies corporate that possess, deal or handle any sensitive personal data or information and* provides for *compensation for failure to protect such data*[68] and Section 72A, which penalizes intentional personal data breach were incorporated.[69] The amendment however did not provide for distinct definitions of personal data or sensitive personal data. Section 43A provided that 'sensitive personal data or information' would mean such personal information as would be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Rule 3 of the Data Protection Rules provides an exhaustive list of eight types of personal data as sensitive personal data: i) password; ii) financial information such as bank account or credit card or debit card or other payment instrument details; iii) physical, physiological and mental health condition; iv) sexual orientation; v) medical records and history; vi) biometric information; vii) any detail relating to the above clauses as provided to body corporate for providing service; viii) any of the

[67] Explanation (i), S. 43A, Information Technology Act, 2000.
[68] S. 43A, Information Technology Act, 2000.
[69] S. 72A, Information Technology Act, 2000.

information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.[70]

The limited scope of 'sensitive personal data or information' is an additional limitation. As technology like the IoT, facilitates ubiquitous data collection, other sensitive personal information such as location, habits, and activity among others should be encompassed by the purview of these Rules.[71]

Rule 6 provides for disclosure of sensitive personal data with prior permission.[72] There is ambiguity regarding regulation for disclosure of non-sensitive personal data. Being in an era of IoT, where sensitive personal data can be derived out of any available non-sensitive personal data, the purpose of this rule seems futile.

2. Personal Data Protection Bill, 2019

With the profound necessity to regulate how personal data should be processed and stored and the procedure on who can and how to access the personal data of the consumers/citizens, the PDP was introduced in the Parliament on December 11, 2019. A framework on people's rights on their personal data is also provided in the Bill.

'Consent' is the paramount prerequisite that must be achieved before accessing any kind of data of the citizens. The Bill does not provide a clear definition of 'consent' or 'explicit consent'. The Bill furnishes a diverse circumstance where consent is not required for data processing of individuals. When there is strict necessity for the State, even the explicit consent required to access sensitive personal data can be overlooked. Consent is the only exception which when taken the citizen's right to privacy claim can be defended against. The Bill confers unrestricted power

[70] Rule 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[71] S. Basu & R. Malik, *Big Data: A Challenge to Data Protection?,* India Law Journal, available at https://indialawjournal.org/big_data_a_challenge_to_data_protection.php, last seen on 10/11/2020.
[72] Rule 6, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

on the state to access individual data which goes against the spirits of landmark 'right to privacy' ruling of the Supreme Court of India.[73]

The application of the Bill extends to the (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India.[74] For the first time, the government is regulated under a bill with respect to data processing. But the main concern is that Section 98 of the Bill gives power to the central government to issue directions in certain circumstances to exempt any governmental agency from complying with the provisions of the Bill.[75] Wherever the Central Government is satisfied that it is necessary in the interest of sovereignty and integrity of India, the security of the State, public order, friendly relations with foreign states, it can direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data.[76] Further, the Government can access the personal data in the interest of wide reasons provided in chapter 8 of the Bill. The exemptional power vested with the government is very broad, leaving scope of misuse and misinterpretation of the same.[77] Surveillance of the citizens can be done legally under the Bill which impacts their freedom of speech, expression and association. Thus, the provision negates the purpose of regulating data processing by the government.

Even though, the Bill's scope is remarkably outstretched, it is the minute details that undermines the main purpose of protecting the rights and interests of the citizens, which must not be overlooked. In fact, the

[73] R.V. Anuradha, *Why the Personal Data Protection Bill spells trouble for India's IT sector*, CNBC TV 18 (01/08/2018), available at https://www.cnbctv18.com/views/why-the-personal-data-protection-bill-spells-trouble-for-indias-it-sector-402301.htm, last seen on 11/11/2020.

[74] S. 2, Personal Data Protection Bill, 2019 (pending).

[75] S. 98, Personal Data Protection Bill, 2019 (pending).

[76] M. Mandavia, *Data Protection Bill: Centre has the power to exempt any government agency from application of act,* Economic Times Government (10/12/2019), available at https://government.economictimes.indiatimes.com/news/policy/data-protection-bill-centre-has-the-power-to-exempt-any-government-agency-from-application-of-act/72456626, last seen on 16/12/2020.

[77] S. Katarki, N. Viswanath , I. Chatterjee & R. Reddy, *The Personal Data Protection Bill, 2019: Key Changes And Analysis*, Mondaq (06/01/2020), available at https://www.mondaq.com/india/privacy-protection/880200/the-personal-data-protection-bill-2019-key-changes-and-analysis, last seen on 11/11/2020.

provisions under the Bill are not free from ambiguity which again provide unfettered powers to the state while defending its preposterous acts.

3. CPA and Consumer Protection (E-Commerce) Rules, 2020.

Through Section 2(7) of the CPA the government widened the definition of 'consumer' by inserting explanation (b) which states that, *"the expressions 'buys any goods' and 'hires or avails any services' includes offline or online transactions through electronic means or by teleshopping or direct selling or multi-level marketing."*

Section 2(47) of the CPA provides the definition of 'unfair trade practice' which states that, "*a trade practice which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice.*" The Section further includes a set of practices which constitutes 'unfair trade practice'. Clause (ix) of sec. 2(47) states that, *"disclosing to other person any personal information given in confidence by the consumer unless such disclosure is made in accordance with the provisions of any law for the time being in force."*

Even though, the Act has made an effort to restrict the misuse of consumer's personal information for the purpose of any kind of trade practices, it fails to give clarity on the aspects of consent of the consumers and sensitivity of the information. Considering the flourishing e-commerce activities, personal data of the consumers like location, mobile number, etc., are the most primitive requirements to avail the e-commerce services. The current data protection law i.e., Data Protection Rules does not include such primitive information as sensitive, thus leaving scope for misuse of the same.

The Consumer Protection (E-Commerce) Rules, 2020 has not touched upon the protection of the data and personal information provided by the consumer, especially when that information is also being accessed out of the country. Absence of specific guidelines regarding personal data under the rules has resulted in ambiguity which affects the compliance of the provisions under Sec. 2(47) of the CPA.

VI. OBSERVATIONS AND SUGGESTIONS

1. Extent of Consent

A raising issue which needs to be addressed is to determine the extent of consent given by the consumers while availing E-services. A framework[78] was released by the Government of India under the department of Ministry of Electronics and Information Technology and Department of Science & Technology in 2012. The main theme of the framework was focused on the necessity for a combined regulation to manage consent issues of a consumer.

Electronic consent is the digital equivalent of a physical letter of permission given by the user which, when presented, allows the data provider to share information regarding the user with a data consumer, for a particular purpose. Electronic consent allows for data to be electronically and securely shared with service providers on an as-needed basis, while maintaining traceability, to ensure that the data trails can be audited in the future. 'Consent' under the PDP must be defined with precision. In order to address the wide scope of situations while getting the consent of the e-service consumers, a set of rules must be framed. Procedural guidelines for exceptional cases where the consent may not be taken must be strictly formulated.

Thus, the government, being procured with the status to manage the country through law can give the status of statutes to mere frameworks, making it mandatory for the companies and other functionaries to follow it. E-consent management must be regulated precisely, since these are the upcoming issues for a modern democracy and a developing country in cyber era.

2. Determining whether a User is a Consumer or not?

The foremost observation is that whether a user of social network websites, apps and messaging platform is a consumer or not. With the increasing

[78] *Electronic Consent Framework - Technology Specifications (Ver 1.1)*, Ministry of Electronics and Information Technology, available at http://dla.gov.in/sites/default/files/pdf/MeitY-Consent-Tech-Framework%20v1.1.pdf, last seen on 11/11/2020.

usage and dependence on such platforms, there is no single person who does not use those. According to Facebook, social media is its product and it enables us to connect with people who matter, wherever they are in the world.[79] A user can not be a consumer if he/she does not pay for a product or service. Anything for free does not entitle the user as a consumer. But most of the social network websites, apps and messaging platform make profits by selling personal data of its users and moreover, they offer their services or facilities for free. A user has to sign in and create an account, thus entitled to use the application. But there are numerous cases and allegations against such platforms for misusing the data of its users. For instance, Facebook is 'free', but we pay with our personal information. That information is then used to sell targeted advertisements- the primary way Facebook makes money.[80] In the case of e-governance services, the determining factors concerning when the citizens will come to be consumers need to be demarcated. The conundrum regarding what constitutes services irrespective of whether consideration fee is demanded or not for availing e-services must be meticulously specified. The personal information received from the citizens like Aadhaar number, PAN, etc., which in turn possesses sensitive personal information must be regarded as the payment for services provided by the government through e-services.

Thus, the users cannot pay their privacy in return of service they avail. Privacy is an immeasurable asset. These platforms act like middlemen alone. Once they collect and sell the data, their business is over. What happens to such data is unknown. Thus, for all the innocent users, the only way of justice is to ascertain or fix their status.

3. Regulation of Anonymized and Pseudonymized Data

Many websites and applications claim that the data they collect is anonymized. Companies and governments both routinely collect and use

[79] B. Gilbert, *Facebook just published a message for its users: No, you're not the product,* Business Insider (23/04/2018), available at https://www.businessinsider.in/tech/facebook-just-published-a-message-for-its-users-no-youre-not-the-product/articleshow/63887171.cms, last seen on 16/12/2020.
[80] Ibid.

our personal data. Data is 'sampled' and anonymized, which includes stripping the data of identifying characteristics like names and e-mail addresses, so that individuals cannot, in theory, be identified. After this process, the data's no longer subject to data protection regulations, so it can be freely used and sold to third parties like advertising companies and data brokers.[81] This whole process is called as de-identification of data.

But in reality, such data can be reidentified. One can never escape from the harsh realities of Big Data. Such data which can be reidentified is called as pseudonymized data. According to a class action lawsuit[82] levied against the social media giant in January 2014, Facebook raked in USD 2.7 billion in sales for helping create targeted ads for companies based on the information its members posted online. While Facebook says the allegations are a myth and promises that it doesn't share personal information and never will, the Facebook Statement of Rights and Responsibilities sings a slightly different tune: It states that Facebook can and will sell personal information – once it's been anonymized.[83]

In 2016, journalists re-identified politicians in an anonymized browsing history dataset of 3 million German citizens, uncovering their medical information and their sexual preferences. The Australian Department of Health publicly released de-identified medical records for 10% of the population only for researchers to re-identify them 6 weeks later.[84] Researchers were able to uniquely identify individuals in anonymized taxi

[81] Imperial College London, *Anonymizing personal data 'not enough to protect privacy,' shows new study,* ScienceDaily (23/07/2019), available at <www.sciencedaily.com/releases/2019/07/190723110523.htm>., last seen on 07/11/2020.

[82] Mathew Campbell and Michael Hurley v. Facebook, Inc, 17-16873 (9th Cir) (2017, U.S. Court of Appeals), available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1611&context=historical, last seen on 07/11/2020.

[83] J. Curtis, *What Are Big Data Analytics and What Does It Mean for Consumers?*, available at https://www.moneycrashers.com/big-data-analytics-consumers/, last seen on 06/11/2020.

[84] C. Culhane, B. I. P. Rubinstein & V. Teague, *Health data in an open world*, Cornell University (15/12/2017), Preprint available at https://arxiv.org/abs/1712.05627, last seen on 06/11/2020.

trajectories in New York City,[85] bike sharing trips in London,[86] and mobile phone and credit card datasets.[87]

Thus, the entire act is like a circle. It's a process where data is claimed to be de identified, but later reidentified to be used for profits. Anonymized data still carries potential to reveal personal information. Hence, modern tools can be developed which forbid companies and other institutions to re identify anonymized information for safety and security concerns of an individual. Also, stringent data regulation policies are necessary to regulate pseudonymized data, the functionaries who are allowed to use it and situations under which pseudo anonymization could take place. Since this is one of the ways through which Big Data is sourced, it is necessary to regulate the same. An example of Facebook holds good for numerous other websites and applications of companies, tele medicinal apps and so on, where it is promised of not selling personal information, but later sold off under the disguise of anonymization.

4. Need for Strong Encryption and Protection of Obtained Data

Another observation was the unintentional effect of Big Data on consumers. Various companies mine the data in order to facilitate their business. But they lack in securing such data collected. Poor security systems can also lead to data leak, whose loss cannot be priced. Misconfiguration issues are far too common for the healthcare sector, which already is being pummeled by cyberattacks. One wrong click and tens of thousands to millions of patient records can be breached. Med Evolve was the biggest misconfiguration breach in the last two years. While the company recently began notifying 205,000 patients of the error, a

[85] M. Douriez, H. Doraiswamy, J. Freire & C. T. Silva, *Anonymizing NYC taxi data: does it matter.*?, IEEE Xplore (2016), available at https://ieeexplore.ieee.org/document/7796899, last seen on 07/11/2020.
[86] J. Siddle, *I know where you were last summer: London's public bike data is telling everyone where you've been,* Vartree Blogspot (10/04/2014), available at https://vartree.blogspot.com/2014/04/i-know here-you-were-last-summer.html, last seen on 06/11/2020.
[87] Y. De Montjoye, L. Radaelli, V.K. Singh A. & Pentland, *Unique in the shopping mall: on the reidentifiability of credit card metadata*., 347 Science 536, 539 (2015), available at https://dspace.mit.edu/bitstream/handle/1721.1/96321/UniqueInTheShoppingMall_draft.pdf?sequence=1&isAllowed=y, last seen on 08/11/2020.

security researcher made the discovery in 2018.[88] A group of Long Island providers and Middletown Medical in New York also made a similar mistake this year.[89]

When the professional development system at Arkansas University was breached in 2014, 50,000 people were affected.[90] That's a large number, but compare it with 145 million people whose birth dates, home and e-mail addresses, and other information were stolen in a data breach at eBay that same year.[91] From the perspective of a security professional, protecting Big Data sets is also more daunting. This is partly due to the nature of the underlying technologies used to store and process the information.[92]

Thus, companies must update their databases and avoid misconfigurations. When a company can make the best use of such database, it is an obligation on them to protect and invest upon a security system. Most of the time, it is difficult to trace the actual owner of such databases. Thus, consumers are diminished from the opportunity to sue and get justice, when a potential threat to their privacy arises. Thus, the issue of ascertaining the owners of such websites must be taken up by amendments, while registering companies under their respective company incorporation acts. Also, companies and other associated functionaries must include data and security researchers in their organization to constantly have a tab on the collection and protection system of data.

5. Consumer Awareness and Need for Self-Management

Self-management of online privacy seems particularly important as the law only provides limited privacy protection. First, in many countries, the law

---

[88] *More than 200,000 patients' records were exposed on MedEvolve's public FTP server – researcher,* DataBreaches.net (16/05/2018), available at https://www.databreaches.net/more-than-200000-patients-records-were-exposed-on-medevolves-public-ftp-server-researcher/, last seen on 16/12/2020.

[89] Supra 39.

[90] J. Ryoo, *Big Data Security Problems threatens consumer privacy,* Government Technology (24/05/2018), available at https://www.govtech.com/data/Big-Data-Security-Problems-Threaten-Consumers-Privacy.html#:~:text=When%20the%20professional%20development%20system,at%20eBay%20that%20same%20year, last seen on 16/12/2020.

[91] J. Ryoo, *Big data security problems threaten consumers' privacy*, The Conversation (23/03/2016), available at https://theconversation.com/big-data-security-problems-threaten-consumers-privacy-54798, last seen on 05/11/2020.

[92] Ibid.

is not fully prepared for modern data processing practices. Even if lawmakers and regulators want to protect privacy, they are struggling with the question of how to provide effective legal privacy protection. Moreover, even if up-to-date privacy laws are in place, enforcement is often insufficient. Regulators have limited resources to make companies comply with the law.[93]

"People value their informational privacy", yet *"they surrender it at the drop of a hat"* by readily sharing personal data in the course of simple daily transactions.[94] Most of the time, consumers online accept to the terms and condition without reading it, and provide their personal information without familiarizing with the privacy policy of such companies. This act of theirs is considered as an informed consent. Companies do mention their intention to utilize the personal information for other purposes of business under such a policy. Thus, the consumers literally give their informed consent for their data to be sold or used for other ulterior purposes.

This means that laws mainly focus on consumers' consent, and lawmakers appear to assume that empowered consumers can make rational, educated decisions in their own best interest. The question, however, is whether people are actually empowered and able to make decisions about giving consent and to protect their online privacy after giving consent. When this would not be the case, it would suggest a need for more effective privacy laws, which rely less on empowering consumers, and more on protecting them.[95]

The paradox, he observes, can be resolved by noting that as long as people do not expect that the details of their health, intimacies and finances among others will be used to harm them in interaction with other people, they are content to reveal those details when they derive benefits from the

[93] Sophie C. Boerman, Sanne Kruikemeier, Freidrik J*, Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data,* Sage Journals, 1, 2 (2018), available at https://journals.sagepub.com/doi/full/10.1177/0093650218800915, last seen on 16/12/2020.
[94] R. A. Posner, *Privacy, Surveillance, and Law*, 75 The University of Chicago Law Review, 245, 251 (2008), available at https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5655&context=uclrev, last seen on 08/11/2020.
[95] Supra 93.

revelation.[96] Thus, consumers should read the policies before consenting to it. Modern consumers, though being well aware about ongoing privacy and data issues must take a step forward in self-regulating their actions.

VII. CONCLUSION

In the present digital and technological era, the roles of the public and private sectors have broadened alongside the increased demands for improved and efficient services from the consumers. The private sector players in order to establish broad customer bases and to achieve profits, collect, store and process the personal information of the consumers to analyze existing and evolving trends. Similarly, the government has inculcated e-services as a part of better and reformed governance. To achieve competent, productive and effective governance, the government needed to take advantage of the technology. Big Data analytics was the solution that both private and public sector players instilled as an integral part of their services.

The benefits of Big Data are being harnessed at every stage and aspect of the service providing process. In the process of gathering different sets of data to coordinate services in a proper, smooth, quick, and effective manner, the most intrinsic right of the citizens i.e., privacy was forgotten. Consent of the citizens and the gravity of its requirement has been overlooked. Lack of specific regulation contributes to the negligence regarding consent.

With new challenges being built on, it has become difficult to cope with evolving technological advances. A specific legislation which is explicit regarding the aspects of consent, the wide scope of definition of consumer, precise regulation on anonymized and pseudonymized data is the need of the hour. The government must also keep the changing technological developments on Big Data and the possible impact the consumers in mind while formulating a specific regulation on Big Data analytics.

[96] Supra 52.

SHORT ARTICLES

THE NEW CONSUMER PROTECTION LAW AND ITS IMPACT ON THE MEDICAL DEVICE REGULATORY FRAMEWORK

[*]Shreya Shenolikar & [**]Darren Punnen

ABSTRACT

India's new consumer protection legislation, the Consumer Protection Act, 2019 ("CPA, 2019") has had a significant impact on all industries, from consumer goods to real estate, and the medical device industry is no exception. However, the industry is uniquely placed in comparison to other mainstream sectors such as automobiles and consumer goods, in that the industry is already regulated under a special legislation i.e., the Medical Device Rules, 2017 ("MDR"). In this paper, we have provided an overview of the CPA, 2019 and the MDR, and the areas in which they overlap. By undertaking this comparison, we aim to understand the combined impact of these regulations on the medical device industry. Further, we have identified areas where there may be conflict between the CPA, 2019 and the MDR and proposed appropriate solutions for such situations.

I. INTRODUCTION

The Consumer Protection Act, 2019 ("**CPA, 2019**"), which replaced the Consumer Protection Act, 1986 (**"CPA, 1986"**) as of July 2020, has become the primary consumer protection legislation in India.[1] The CPA, 2019 is considerably more comprehensive than its predecessor and a revamp of the law had been much awaited, considering the numerous developments that have taken place over the three decades since the enactment of the CPA, 1986. The increasing reliance of technology in

[*] Shreya Shenolikar, Member, Pharma & Life Sciences Practice, Nishith Desai Associates.
[**] Darren Punnen, Senior Member, Pharma & Life Sciences Practice, Nishith Desai Associates.
They acknowledge the assistance by Ms. Anjuri Saxena, IV Year Student, Rajiv Gandhi National University of Law, Punjab.
[1] Ministry Of Consumer Affairs, Food And Public Distribution, Government of India, *Consumer Protection Act, 2019*, available at http://egazette.nic.in/WriteReadData/2020/220546.pdf, last seen on 16/01/2021; Ministry Of Consumer Affairs, Food And Public Distribution, Government of India, available at http://egazette.nic.in/WriteReadData/2020/220657.pdf, last seen on 16/01/2021.

everyday life as well as the introduction of several healthcare products intended for direct use by consumers had called for greater accountability of companies operating in these sectors.

A more specific product liability regime as well as a consumer authority were, therefore, welcome introductions to the CPA, 2019. There are now specific provisions addressing product liability and delineates when the product manufacturer, product seller and product service provider would be held liable to pay compensation for any harm caused by a defective product manufactured by a product manufacturer, serviced by a product service provider or sold by a product seller.[2]

The CPA, 2019 also establishes the Central Consumer Protection Authority (**"CCPA"**) as the regulator responsible for protecting consumer rights.[3] This includes enforcing the rights of consumers as a class, preventing unfair trade practices and ensuring that no false advertisements are made in respect of goods and services.[4] The CCPA also has the power to initiate product recalls and initiate an inquiry or investigation into alleged violations of consumer rights or unfair trade practices either on its own initiative or based on a complaint received from consumers.[5]

The CPA, 2019 applies to all goods and services unless specifically exempted by the Central Government.[6] No goods or services have been excluded so far. As a result, the CPA, 2019 also applies to medical devices. It should be noted here that medical devices are specifically regulated under a specific regulatory framework i.e., the Medical Device Rules, 2017 ("**MDR**") administered by the Central Drugs Standard Control Organization (**"CDSCO"**).

Due to this, there is some overlap in the functions exercised by the CCPA and the CDSCO in respect of medical devices. In this article, we have attempted to provide an overview of the applicable regulatory framework

[2] Chapter VI, The Consumer Protection Act, 2019; S. 82, The Consumer Protection Act, 2019.
[3] Ministry of Consumer Affairs, Food and Public Distribution, Government of India, available at http://egazette.nic.in/WriteReadData/2020/220659.pdf, last seen on 16/01/2021, last seen on 16/01/2021; S. 10, The Consumer Protection Act, 2019.
[4] S. 18, The Consumer Protection Act, 2019.
[5] S. 18 (2), The Consumer Protection Act, 2019.
[6] S. 1 (4), The Consumer Protection Act, 2019.

under the CPA, 2019 and MDR, examine the overlap between the two regulations and chart a way forward. The article begins by outlining the overlapping provisions under the CPA, 2019 and MDR in respect of medical devices as well as the overlapping duties, powers and responsibilities of the CCPA and CDSCO in relation to medical devices. Subsequently, it examines the impact of such overlapping provisions on the medical device industry and argues that in cases of such overlap, the MDR should supersede. Finally, it provides inputs on the way the legal framework should adapt to best accommodate the welfare of consumers and minimize ambiguities in enforcement mechanisms.

II. OVERLAP BETWEEN THE CPA, 2019 AND THE MDR

The CPA, 2019 and MDR were enacted with different intentions in mind. The CPA, 2019 was enacted to provide consumers with a direct remedy in the event the consumer receives a defective product or in case of an unfair trade practice. On the other hand, the MDR is intended as a more specific regulation that governs various aspects of medical devices, including its safety and efficacy. The MDR broadly sets out standards required to be followed by manufacturers/importers of medical devices and requires manufacturers, importers and sellers of medical devices to obtain the requisite licenses prior to undertaking the respective activities.

1. Product Liability

The term 'product liability' is specifically defined under the CPA, 2019 but not under the MDR.[7] Nonetheless, both the CPA, 2019 and the MDR have similar provisions dealing with liability arising out of any harm caused by a defective product. Under the CPA, 2019, product liability is defined as the *"responsibility of a product manufacturer or product seller, of any product or service, to compensate for any harm caused to a consumer by such defective product manufactured or sold or by deficiency in services relating thereto"*.[8]

[7] S. 2 (34), The Consumer Protection Act, 2019.
[8] Ibid.

The CPA, 2019 divides responsibility between the product manufacturer,[9] product seller[10] and product service provider[11].[12] Broadly, the liability is divided based on the entity who is directly responsible for causing the damage. For instance, the product manufacturer is responsible in cases of manufacturing defects, if the product is defective in design or does not conform to express warranty. [13] The product seller is liable in cases where the seller has modified the product or made an express warranty independent of a manufacturer's warranty. [14] The product service provider is liable if the service provided was not as per standards set out in law or contract. All three parties are liable in the event adequate instructions for usage were not provided. [15]

Corresponding provisions in relation to medical devices are captured under the Drugs and Cosmetics Act, 1940 (**"D&C Act"**) – the parent legislation under which the MDR is framed. The D&C Act criminalizes the import, manufacture and sale of medical devices which are (i) not of standard quality, (ii) adulterated, misbranded or spurious, and (iii) otherwise prohibited under law.[16] In the event the above-mentioned provisions are violated, the manufacturer or importer of the medical device, as the case may be, would be held liable.

It should be noted that an amendment has been proposed to the MDR under which manufacturers/importers of medical devices would be held liable in the event a medical device is found malfunctioning or not in compliance with the conditions of the license to manufacture/import granted to the manufacturer/importer, as the case may be (**"Compensation Amendment"**).[17] This compensation would likely be

[9] S. 84, The Consumer Protection Act, 2019.
[10] S. 86, The Consumer Protection Act, 2019.
[11] S. 85, The Consumer Protection Act, 2019.
[12] The term 'product service provider' is distinct from 'service provider' under the Consumer Protection Act. Unlike a service provider who provides a service in general, the product service provider provides any service in respect of a product e.g., repairs and maintenance.
[13] Supra 9.
[14] Supra 10.
[15] Supra 11.
[16] Ss. 10 and 18, The Drugs and Cosmetics Act, 1940.
[17] Minutes of the 81st Meeting of Drugs Technical Advisory Board, Central Drugs Standard Control Organization, available at

payable to the aggrieved patient (in case of injury) or the legal heirs of the patient (in case of death). The Drugs Technical Advisory Board (**"DTAB"**) – the apex body relating to technical matters in respect of drugs and medical devices – had constituted a sub-committee under the chairmanship of Dr. B.D. Athani (**"Sub-Committee"**) which is currently in the final stages of preparing its report. The Sub-Committee was constituted to examine the issue of compensation in case of faulty medical devices and present its report to the DTAB. The Sub-Committee Report reportedly recommends the establishment of a 'causality assessment committee' to determine the quantum of compensation.[18]

From the above, it can be seen that the broad grounds for holding a manufacturer liable are similar under the CPA, 2019 and MDR i.e., the product is defective in that it does not adhere to the standards required to be maintained in respect of the product under law or contract. Nonetheless, there are a few differences between the two regulations in respect of product liability, as follows:

1.1 Entity Responsible

While both the CPA, 2019 and the MDR hold the manufacturer responsible in product liability claims in some instances, the CPA, 2019 has an additional component where the product seller or product service provider may also be held liable in a product liability claim.

The MDR at present does not contain provisions under which the product service provider may be held liable. Product sellers under the MDR could be held liable in limited instances only (primarily for violation of license conditions).[19]

https://cdsco.gov.in/opencms/opencms/system/modules/CDSCO.WEB/elements/common_download.jsp?num_id_pk=NTY2, last seen on 16/01/2021.

[18] T. Thacker, *Side effects of medical devices: Panel chalks out formula for compensation*, The Economic Times (26/09/2019), available at https://economictimes.indiatimes.com/industry/healthcare/biotech/healthcare/side-effects-of-medical-devices-panel-chalks-out-formula-for-compensation/articleshow/71303722.cms?from=mdr, last seen on 16/01/2020.

[19] See Rules 30 and 38, The Medical Device Rules, 2017.

1.2 Who Can Initiate Action?

Generally, only a consumer (including consumer associations) can bring an action under the CPA, 2019.[20] It may be noted here that individuals are not deemed to be consumers under the CPA, 2019 in cases where they have purchased a good or used a service for commercial purposes, unless such individuals purchase a good or use a service solely for self-employment purposes of earning their livelihood.[21] Therefore, commercial establishments such as clinics and hospitals may not eligible to bring an action in consumer court in the event they receive a defective device.

On the other hand, any person can approach the relevant licensing authority to file a complaint in respect of a faulty medical device.[22]

1.3 Manner of Initiating Action

Under the CPA, 2019 the consumer has a direct claim against the manufacturer and if held liable, the manufacturer is required to directly compensate the consumer for harm or injury caused.[23] To initiate an action in a product liability claim, the consumer should file a complaint before the appropriate consumer forum where it will be adjudicated upon thereafter.

Under the D&C Act and MDR[24], any person who is aware of a defect in a medical device may approach the CDSCO (or any of the state-level licensing authorities (**"SLA"**) functioning under the CDSCO) to file a complaint. Following this, the CDSCO or the SLA will take action against the faulty medical device manufacturer/importer as it deems fit. This may include conducting raids or other inquiry or investigation,[25] issuing show cause notices to the relevant manufacturer/importer,[26] suspending or cancelling[27] the licenses held by the manufacturer/importer to restrain from carrying out business operations in India, and even initiating criminal

[20] S. 35, The Consumer Protection Act, 2019.
[21] S. 2 (7), The Consumer Protection Act, 2019.
[22] Rule 70 (vi), The Medical Device Rules, 2017.
[23] S. 82, The Consumer Protection Act, 2019.
[24] Rule 70, The Medical Device Rules, 2017.
[25] Rule 20 (8), The Medical Device Rules, 2017.
[26] Rule 33 (1), The Medical Device Rules, 2017.
[27] Rule 30, The Medical Device Rules, 2017.

proceedings[28] against such manufacturer/importer in a court of law. A portion of the fine imposed by the court may be directed to be paid to the affected person/legal heir. Therefore, while the ambit of persons who can make a complaint is wider than that under the CPA, 2019 the remedies available are in the nature of penal action that does not provide compensation/restitution to the complainant or other aggrieved party.

2. Product Recall

A product recall broadly refers to the process of the manufacturer/importer of a good, taking back goods that are already present in the market at different levels of the supply chain.[29] The recall usually takes place due to a deficiency in the product discovered after the good was already dispatched from the manufacturer's warehouses. A recall may be voluntary (initiated by the manufacturer/importer) or statutory (a recall directly be a regulatory/statutory authority).

Both the CPA, 2019 and the MDR have provisions relating to product recall. Under the CPA, 2019, the CCPA has the power to recall goods from the market which are hazardous, dangerous or unsafe.[30] At the moment, the CPA, 2019 does not specifically cover voluntary recalls. There is also no specific process prescribed in case of statutory recalls initiated under the direction of the CCPA. Further, given that the recall provision was not present under the CPA, 1986, there is little precedent on how a product recall should be conducted or who would be responsible for conducting such recall.

The MDR contains a skeletal procedural outline for both voluntary and statutory recalls of medical devices.[31] The MDR defines recalls as follows:

> any action taken by its manufacturer or authorized agent or supplier to remove the medical device from the market or to retrieve the medical device from any person to whom it has been supplied, because the medical device, —

[28] S. 22 (2), The Drugs and Cosmetics Act, 1940.
[29] Guidelines on Recall and Rapid Alert System For Drugs (Including Biologicals & Vaccines), Central Drugs Standard Control Organization, CDSCO/RRAS, (23/11/2012) available at https://cdsco.gov.in/opencms/export/sites/CDSCO_WEB/Pdf-documents/biologicals/4GuidelineRecalRapidAlert.pdf, last seen on 16/01/21.
[30] S. 20, The Consumer Protection Act, 2019.
[31] Rule 3 (zp), The Medical Device Rules, 2017.

(a) is hazardous to health; or
(b) fails to conform to any claim made by its manufacturer relating to its quality, safety or efficacy; or
(c) does not meet the requirements of the Act and these rules

Under the MDR, the manufacturer (in case of domestic goods) and the authorized agent of the foreign manufacturer (in case of imported goods) are responsible for the recall. The manufacturer/authorized agent is also required to inform the Central Licensing Authority (CDSCO) or the SLA in the event a medical device which may be unsafe for patients has been placed on the market.[32] The recalled medical devices are required to be destructed under the supervision of the Central Licensing Authority (CDSCO) or the SLA.[33]

The MDR comprises a product-specific process for recall while the CPA presently only provides a power to the CCPA to initiate product recall. Further, the MDR also comprises post-recall procedures on the destruction of the recalled medical devices.

3. Pricing

Medical devices are considered to be essential commodities and their prices are regulated under the Drugs (Prices Control) Order, 2013 (**"DPCO"**) administered and enforced by the National Pharmaceutical Pricing Authority (**"NPPA"**). The DPCO directly or indirectly regulates the prices of all medical devices. The NPPA fixes the ceiling price of medical devices considered to be essential (knee implants and cardiac stents are presently the only two devices in this category).[34] For all other devices, the manufacturers/importers are required to ensure that the price of such device does not increase by more than 10% in any given period.[35] All entities along the supply chain are required to display the price list conspicuously.[36] In the event the manufacturers/importers contravene the provisions of the DPCO, the NPPA is empowered to initiate proceedings

[32] Rule 26 and 38, The Medical Device Rules, 2017.
[33] Rule 80 (2), The Medical Device Rules, 2017.
[34] Rule 4 r/w 14, The Drugs (Prices Control) Order, 2013.
[35] Rule 20, The Drugs (Prices Control) Order, 2013.
[36] Rule 24 (3), The Drugs (Prices Control) Order, 2013.

against such manufacturer/importer and required the person to deposit the overcharged amount with the NPPA.[37]

The CPA, 2019 does not prescribe prices of any commodity. Nonetheless, charging a price higher than the one displayed on the good, fixed by law, or displayed on a price list exhibited by a trader as required under law is grounds for a complaint under the CPA, 2019.[38] As a result, in the event any entity along the supply chain of a medical device charges a price higher than one displayed on the medical device/the price list or higher than the maximum price that may be fixed in respect of such medical device under the DPCO, the consumer has a right to directly proceed against such entity.

The key takeaway here is that in the event of overcharging, the CPA, 2019 provides a direct remedy to the consumer to claim for the overcharged amount from the responsible entity. The DPCO, on the other hand, empowers the NPPA to commence proceedings against the manufacturer/importer of the good in respect of the overcharged amount.

III. THE WAY FORWARD

As can be seen from the previous section, the CPA, 2019 essentially gives the consumer a direct claim against the manufacturer/importer of a medical device in product liability and overcharging cases. In recall cases, the powers of the CCPA overlap with those of the CDSCO/SLA.

While providing consumers with a direct remedy against the manufacturer/importer may initially seem conducive to justice, it may create inequities from the perspective of the medical device manufacturer/importer. Some of the key considerations here are as follows:

1. Dual Penalty

In each of the above cases, the relevant regulatory authority (CDSCO/SLA/NPPA) has a separate right to initiate proceedings against the medical device manufacturer/importer while the consumer has a

[37] Rules 14, 15, 16 and 20, The Drugs (Prices Control) Order, 2013.
[38] S. 2 (6) (iv), The Consumer Protection Act, 2019.

separate claim. Due to this, two parallel claims arising out of the same set of facts may be initiated against the medical device manufacturer. As a result, the medical device manufacturer/importer may be held liable twice in respect of the same action. It is pertinent to note here that the nature of the penalty in the majority of the cases is also the same. Except for cases where the CDSCO/SLA initiates criminal prosecution against the medical device manufacturer/importer for manufacturing/importing a medical device that is adulterated, misbranded, spurious or not of standard quality, all penalties are civil in nature.

To elaborate, compensation payable to patient or legal heirs of the patient due to harm arising out of a faulty medical device is civil in nature, both under the CPA, 2019 and as per the recommendations proposed to be made by the Sub-Committee. Due to this, in the event a consumer initiates action before both the CDSCO/SLA and the consumer forum, the medical device manufacturer/importer may be held liable to pay compensation twice. In cases of overcharging, the NPPA may initiate separate proceedings against the manufacturer/importer of the medical device to recover the entirety of the overcharged amount while the consumers who have been overcharged may file several complaints in respect of the same overcharging. As a result of this, medical device manufacturers/importers, who were earlier responsible only to the regulator (who in turn represented the interests of the consumers as a whole) may now be subject to multiple suits in respect of the same set of facts.

To prevent this, it may be good to explore whether medical devices be exempt from the provisions of the CPA, 2019 dealing with overcharging and product liability. Such a move may not harm the rights of consumers as they would continue to have the power to approach the relevant regulator for addressing their grievances. Further, the medical regulatory framework is better suited to addressing such claims as it allows complaints not only from consumers but, also commercial organizations.

In the case of product recall, the CDSCO already has an established procedure for carrying out a medical device product recall. As a result, it is proposed that in the event the CCPA receives a complaint or otherwise

comes to know of a hazardous medical device being present in the market, the CCPA should approach the CDSCO to initiate a statutory recall as contemplated under the MDR. This can be incorporated as internal protocol in the CCPA's governing documents.

2. Nature of Enforcement/Adjudicating Authority

Determining liability in a medical device product liability case requires specialized and technical knowledge. Each medical device has its own medical specialization and adjudicating authorities are required to parse through volumes of evidence on the functioning of the medical device and the facts of each case to arrive at a decision. Matters are further complicated in cases where a determination needs to be made on whether the harm was caused due to a fault in the medical device or due to the faulty application of the medical device by the treating physician. Due to this, consumer forums, which are strapped for time and deal with a variety of matters, may not be best equipped to deal with medical device product liability claims.

The 'causality assessment committee' proposed to be set up under the MDR may be a better fit to determine compensation in case of injuries caused due to a faulty medical device. The Sub-Committee has also reportedly proposed a formula for calculation of compensation which may aid in quicker resolution of cases as compared to the consumer forums.[39]

IV. CONCLUSION

The CPA, 2019 is a significant positive development to ensure that consumers' rights are protected. However, as the CPA, 2019 applies to all industries, goods and services, the legislation may cause an overlap in claims for certain sectors which are already specifically regulated. The medical device industry happens to be one of them.

As a result, at least in clear cases of overlap between the CPA, 2019 and MDR, the provisions of the MDR should ideally take precedence. This will ensure both the protection of consumer rights as well as providing a more conducive business environment for the medical device industry. At the

[39] Supra 18.

CCPA's level, the CPA, 2019 already provides the option for the CCPA to forward any reports of prima facie cases to relevant sectoral regulators. If this option is used liberally, especially with respect to medical device claims, the process may in turn be beneficial for the consumer, as it widens the avenues for a consumer to raise a claim, while also being assured of a more structured process overseen by a sectoral regulator for resolution.

THE BIG GETS BIGGER: THE NEED TO CLOSELY MONITOR THE FACEBOOK-JIO DEAL THROUGH COMPETITION LAW

[*] *Pankhudi Khandelwal*

ABSTRACT

The Competition Commission of India ("CCI") has recently approved the acquisition of minority non-controlling shareholding of approximately 9.99% in Jio Platforms by Facebook. Analyzing this kind of arrangement between the world's largest social media site and the biggest telecom operator in India requires not just the assessment of business aspects of the deal, but also the collection of huge amounts of consumer data by both the entities and raises the concern of protection of such data. Facebook has had a record of acquiring companies to acquire more data of users, which makes it important for the CCI to analyze the deal keeping in mind the dominance of Facebook in the collection of data. The article elaborates on this practice of Facebook by analyzing the Facebook/WhatsApp merger case to argue that the Facebook-Jio deal should be monitored by the competition law authority. This becomes more interesting when we look at the decision of the German Federal Court of Justice decided on the same date as the CCI order which has held that Facebook has abused its dominant position by illegally combining data from various third-party websites. The decision relied on the aspect of consumer choice to examine the behavior of dominant entities and stated that a dominant entity not giving its consumers the choice to decide how much data they want to share causes an abuse of its position. The article discusses the intervention required by competition and consumer protection law to ensure the effectiveness of consumer consent post Facebook-Jio deal.

I. INTRODUCTION

The Competition Commission of India (**"CCI"**) has recently approved the acquisition of minority non-controlling shareholding of approximately 9.99% in Jio Platforms Limited by Facebook's indirect wholly-owned subsidiary, Jaadhu Holdings Limited ("**Jaadhu**") on June 24, 2020 (**"CCI**

[*] Pankhudi Khandelwal, Lecturer, Jindal Global Law School, Sonipat, Haryana.

Order").[1] As per the CCI Order, since the acquisition is of a minority non-controlling stake and Facebook and Jio Platforms will continue to operate independently, it does not alter the competitive landscape in any potential relevant market. However, analyzing this kind of arrangement between the world's largest social media site and the biggest telecom operator in India requires an assessment of the increase in the ability of both the entities to collect huge amounts of consumer data.

The CCI, while looking into the concern of potential data sharing between both the parties, has held that since the acquisition is only of 9.99%, it may not result in unrestricted access to each other's resources including user data. Further, the CCI held that it has been clarified by Jaadhu that data sharing is not the purpose of the acquisition, nor will either side be acquiring ownership of the other's data. However, for implementation of the arrangement, WhatsApp and JioMart will receive or send limited data for the purpose of facilitating e-commerce transactions on JioMart. The purposes for data sharing mentioned under the deal create a potential for misuse of consumer data. Facebook and Jio, both being dominant companies in their respective relevant markets i.e., social media and telecom respectively, have the potential to cause irreconcilable harm to the privacy of consumers. The article tries to analyze how the Facebook-Jio deal should be looked through the lens of competition law to prohibit Facebook and Jio from violating data protection and privacy obligations, especially since India does not have a legislation dealing with the data protection yet.

The article elaborates on the data sharing practice of Facebook by analyzing the Facebook/WhatsApp merger[2] to argue that the recent Facebook-Jio deal should be met with certain skepticism from the competition law authority, which should keep a close watch on the developments that happen as a result of the deal. This becomes more interesting when we look at the recent decision of the German Federal

[1] Jhaadu Holdings LLC v. Jio Platforms, Combination Registration No. C-2020/06/747, (Competition Commission of India, 24/06/2020).
[2] Facebook/WhatsApp Merger Procedure, Case No. COMP/M.7217, 03/10/2014.

Court of Justice,[3] which has held that Facebook has abused its dominant position by combining user data from various third-party websites. This decision has paved the way for competition law authorities to examine the behavior of dominant entities based on their data collection practices.

The article is divided into four parts. Part II of the article analyses the aspects of the Facebook-Jio deal and how the two companies together have the potential to abuse their dominant position. Part III discusses the intervention required by competition and consumer protection law based on the Facebook/WhatsApp merger decision and the measures that can be taken to ensure consumer choice and consent while sharing of data based on the recent Facebook decision by the German Federal Court of Justice. Part IV concludes the work.

II. FACEBOOK-JIO DEAL

Through the acquisition of the largest minority shareholding in Jio, Facebook may have gained the potential to acquire large amounts of consumer data through the combined platform because of huge market shares of both the dominant entities. Under the CCI Order, Jio Platforms, WhatsApp Inc., and Reliance Retail Limited have also proposed to enter into a separate commercial arrangement. JioMart (commerce marketplace by Reliance Retail Limited) plans to integrate certain WhatsApp services with JioMart. While Reliance has been trying to get into the retail market in India, Facebook has been trying to introduce WhatsApp pay through WhatsApp. With Jio's 388 million users and WhatsApp's 400 million users in India,[4] both the companies together can establish a platform which can compete with already established incumbent players of the market, both in the retail sector such as Amazon and Flipkart and e-wallet market such as Paytm, Google Pay etc.

[3] KVR 69/19 (Federal Court of Germany), 23 June, 2020, available at https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020080.html?nn=10690868, last seen on 30/06/2020.

[4] K. Parbat, *Facebook deal gives Jio a good leverage in WhatsApp: Experts*, The Economic Times (23/04/2020), available at https://economictimes.indiatimes.com/tech/internet/deal-gives-jio-a-good-leverage-in-whatsapp/articleshow/75305648.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, last seen on 19/06/2020.

This becomes more concerning as after the Facebook-Jio deal, Jio has been able to attract huge investment by selling minority stakes in the company to various entities.[5] Generally, e-commerce platforms have been known to adopt an initial loss-making strategy to become the dominant entity and exclude competitors through predatory pricing. This strategy works because of the heavy investments that these companies receive. With Reliance Jio gaining so much investment, it is possible for it to exclude competitors while making losses. Jio had earlier used the predatory pricing strategy to enter the telecommunications market. CCI did not hold the practice to be anti-competitive as Jio was not a dominant player at the time.[6]

Further, the approach that is generally taken by CCI while analyzing the claim of predatory pricing is that predatory pricing is harmful only if the entity engaging in such practice can recoup its losses later.[7] Otherwise, it is considered as a legitimate strategy to enter the market. However, it has been seen that companies do not need to recoup the losses because they are backed by heavy funding. Due to their deep pockets, they can continue to dominate in the market with low costs. This could prove to be harmful to other players of the market who do not have that kind of investment. Because of these strategies, the market does not compete on merits anymore, which might push as efficient competitors out of the market. This dominant platform can then be used to collect large amounts of consumer data to make profits from targeted advertising. This in turn would lead to lower choice for consumers as there would be no alternative platform that the consumers would be able to choose from, thus limiting the incentives for the dominant platform to compete on the basis of better privacy policies.

---

[5] *Saudi Arabia's PIF to invest Rs 11,367 crore in Jio Platforms for 2.32% stake*, The Economic Times (18/06/2020), available at https://economictimes.indiatimes.com/markets/stocks/news/saudi-arabias-pif-to-invest-rs-11367-crore-in-jio-platforms-for-2-32-stake/articleshow/76444288.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, last seen on 19/06/2020.

[6] Bharti Airtel Limited v. Reliance Industries Limited, Case no. 3 of 2017 (Competition Commission of India, 05/12/2018).

[7] Transparent Energy Systems (P) Ltd. v. TECPRO Systems Ltd., Case No. 09 of 2013 (Competition Commission of India, 11/06/2013).

One of the other consequences of the deal is the approval of WhatsApp Pay by the National Payments Corporation of India (**"NPCI"**).[8] While NPCI has issued a cap of 30% on the volume of transactions, WhatsApp still has the potential of gaining huge amounts of financial data of consumers along with data on their spending patterns, which it can leverage to other services including using such data for the betterment of Jio services such as Jio mart, thus helping both the parties in further strengthening their dominant position excluding other competitors from the market.

III. INTERVENTION OF COMPETITION AND CONSUMER PROTECTION LAW

The need for intervention of competition law for compliance with data protection obligations can be seen through the WhatsApp/Facebook merger. While assessing the merger, the European Commission did not try to ascertain if Facebook can use data from WhatsApp but instead relied on the undertaking by Facebook that WhatsApp cannot serve as a potential source for data due to different identifiers i.e. an account on Facebook can be created through an E-Mail id, whereas contact number is required to create an account on WhatsApp.[9] However, it was later seen that Facebook had provided misleading information to the Commission, since after the merger, WhatsApp changed its privacy policy to allow sharing of information on WhatsApp to other Facebook family of companies.[10]

When the same practice was challenged before the CCI,[11] it held that data sharing from WhatsApp to Facebook is to improve the experience on Facebook. WhatsApp gave the option to the consumers to delete their WhatsApp account within 30 days if they do not want their data to be shared. Consumers were given an 'all or nothing' option where they had no bargaining power if they wanted to continue using the services of

[8] *NPCI gives approval for WhatsApp to 'go live' on UPI in phased manner*, CNBC (06/11/2020), available at https://www.cnbctv18.com/business/companies/npci-whatsapp-upi-live-7408451.htm, last seen on 19/12/2020.
[9] Facebook/WhatsApp Merger Procedure, Case No. COMP/M.7217, 03/10/2014.
[10] Supra 2.
[11] Shri Vinod Kumar Gupta v. WhatsApp Inc., Case No. 99 of 2016 (Competition Commission of India, 01/06/2017).

WhatsApp with better privacy provisions. The CCI held that users who do not want their data to be shared have the option to delete their Whatsapp account and therefore, it does not constitute an abusive practice. Further, CCI held that breach of privacy fell under the Information Technology Act, 2000 (**"IT Act"**) and so it does not have the jurisdiction to decide violations under the same.

The CCI completely neglected the impact of network effects of WhatsApp. Network effects occur when the value of the platform increases with the increase in the number of users on the platform.[12] Network effects make it difficult for consumers to shift to any other platform even if they do not like the new privacy policy as all their contacts are on the same platform. Therefore, the consumers are left with no option but to accept the privacy policies offered by the dominant platform on an 'all or nothing' basis. Due to this unequal bargaining position between the consumers and the platform, consumers are given no effective choice to negotiate the amount of data that they are willing to share with these platforms. Because of network effects, there is a potential for consumers to become so heavily dependent on the platform created through the Facebook-Jio deal that it does not leave room for any other competitors to enter the market and compete on privacy.

The data of the consumers can be protected under the new Consumer Protection Act, 2019 (**"CPA"**). The CPA establishes a new Central Consumer Protection Authority (**"CCPA"**)[13] which has the right to inquire into violations of consumer rights or unfair trade practices, either *suo motu* or on a complaint received.[14] 'Unfair trade practice' has been defined under the CPA to mean a trade practice which adopts any unfair method or unfair or deceptive practice.[15] The section goes on to give an inclusive list of unfair trade practices. While excessive collection of data is not explicitly mentioned under the definition, the definition is broad enough to include any practices which are unfair for the consumers or violates their rights.

[12] A. Ezrachi & M. E. Stucke, *Virtual Competition: The problems and perils of algorithm-driven economy*, Harvard University Press (2016).
[13] S. 10, The Consumer Protection Act, 2019.
[14] Ibid, S. 18 (2) (a).
[15] Ibid, S. 2 (47).

The CPA also covers providing unfair contracts to the consumers by imposing on the consumer any unreasonable charge, obligation or condition which puts such consumer to disadvantage.[16]

However, while assessing data-driven mergers, it is only the competition law authorities which can assess whether the merger would leave any incentives for the merged digital player to compete on privacy. This is the reason why there is a requirement for competition law to correct the practices of collection and usage of data by dominant companies. The CCI did not intervene in the data collection practices of WhatsApp because it felt that it does not have the jurisdiction to decide issues on privacy. This becomes more problematic since the Personal Data Protection Bill, 2019[17] (**"PDP Bill"**) is yet to be passed. However, even if the PDP Bill is passed, companies can still acquire data through consent given by consumers. However, as seen above, this consent is not always meaningful as consumers are given an 'all or nothing' option.

The jurisdictional issue relating to intervention of competition authorities in data protection obligations of dominant entities and choice provided to consumers regarding usage of their data could be said to be rationalized by the Federal Court of Justice of Germany in its recent decision involving sharing of data by Facebook.[18] The German competition law authority initiated proceedings against Facebook and found that the social networking platform was abusing its market power by violating data protection rules.[19] While this decision was stayed by the Higher Regional Court[20] saying that violation of data protection rules does not fall within the jurisdiction of competition law, the Federal Court of Justice of Germany has rejected this stay and upheld the prohibition imposed by Federal Cartel Office by stating that Facebook was abusing its dominant

[16] Ibid, S. 2 (46).
[17] The Personal Data Protection Bill, 2019 (pending).
[18] Supra 3.
[19] *Facebook Inc. i.a.- The use of abusive business terms pursuant to Section 19 (1) GWB, B6-22/16,* Bunderskartellamt, available at https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5, last seen on 16/12/2020.
[20] J. Gesley, *Germany: Higher Regional Court Suspends Restrictions Placed on Facebook*, Library of Congress, available at https://www.loc.gov/law/foreign-news/article/germany-higher-regional-court-suspends-restrictions-placed-on-facebook/, last seen on 17/12/2020.

position with the terms of use.[21] The decision was based on the fact that the terms do not leave any choice for users between a more personalized experience based on combination of data from different sources or an experience based solely on the data disclosed on Facebook.[22] The decision has given competition law a role that it can play in prohibiting dominant companies from abusing their dominant position by ensuring better privacy policies.

As has been seen from the Facebook-WhatsApp case in India, the present data protection framework in India does not prevent sharing of data between two entities. This becomes more alarming when the issue relates to sharing of data between two of the most dominant entities. In the CCI order, on the aspect of potential data sharing between the parties, the CCI has held that since the acquisition is only of 9.99%, it may not result in unrestricted access to data. The CCI has relied on the submission of the parties that data sharing is not the purpose of the acquisition. However, the arrangement still raises questions as WhatsApp and JioMart will receive or send limited data for the purpose of facilitating e-commerce transactions on JioMart.

It must be noted that similar commitments were given by Facebook during the Facebook/WhatsApp merger.[23] From the past experience, it can be speculated that Facebook would try to benefit from the data that Jio has on consumers. Even if data sharing is not the purpose of acquisition and it has been committed by Facebook that the data sharing will be limited, there is ambiguity with respect to how much sharing of data is limited. While the General Data Protection Regulation (**"GDPR"**) in Europe or the PDP Bill in India provide for principles such as minimization in collection of data[24]

---

[21] J. Dreyer, A. Köhler & K. Pauls, *Germany: Federal Court summary judgment: FCO achieves stage victory against Facebook*, Privacy Matters, DLA Piper (25/06/2020), available at https://blogs.dlapiper.com/privacymatters/germany-federal-court-summary-judgment-fco-achieves-stage-victory-against-facebook/, last seen on 27/06/2020.

[22] R. Polley, L. M. Baudenbacher, R. Kaup & F. A. Konrad, *German Federal Court of Justice Provisionally Finds Facebook's Data Collection Practices Abusive*, Cleary Gottlieb, available at https://www.clearygottlieb.com/-/media/files/alert-memos-2020/german-federal-court-of-justice-provisionally-finds-facebooks-data-collection-practices-abusive.pdf, last seen on 01/07/2020.

[23] Supra 2, Facebook / WhatsApp merger.

[24] Art. 5 (1) (c), The General Data Protection Regulation, 2016 (European Union).

and collection of data in a fair and reasonable manner,[25] there is still no objective criteria to ascertain what amount of data is limited or necessary for the purpose mentioned by the parties. Therefore, even if Jaadhu and Jio will not be owning each other's data in entirety, they can still make use of the shared data to the detriment of the consumers.

The CCI order states that any anti-competitive conduct resulting from any data sharing in the future could be taken up by the Commission under Section 3[26] and/or Section 4[27] of the Competition Act, 2002 having due regard to the dynamics of the concerned markets and position of the parties. However, the CCI in the present case could have taken certain commitments from the parties with respect to data sharing in more objective terms as was done by the European Commission in the Facebook/WhatsApp merger. The purpose mentioned by the parties, i.e., "*purposes connected with RJIO's business operations*", is too broad as it could include, among other things, usages that users may consent to even if it is not absolutely essential for purposes connected with business operations. As has been seen above, due to the unequal bargaining position of the consumers, the platforms can take consent from the consumers for sharing of huge amounts of their data without giving them any choice as to what data they actually want to share. This can be a cause for potential harm to the personal data of the consumers.

However, since the CCI has not taken into account the potential harm that can be caused due to the deal, it is important that the CCI keeps a close watch on the developments from the deal, especially, due to the limitations of the data protection law in India. As a result, it becomes necessary that CCI intervenes at the right time to the extent necessary to correct any abusive practices that the platform might be indulging in, post the merger. This would require active monitoring on the part of CCI.

[25] The Personal Data Protection Bill, 2019 (Draft Bill 2018).
[26] S. 3, The Competition Act, 2002.
[27] Ibid, S. 4.

IV. CONCLUSION

As demonstrated from the above discussion, robust regulatory oversight over the recent Facebook-Jio deal is required since the acquisition has the potential of misusing consumers' data and causing irreconcilable harm. Consumers need to be provided with a choice on the amount of their data that the companies should be allowed to collect and use. As per the CCI Order, through JioMart, Reliance wants to connect customers with Kirana stores and other small and micro local Indian businesses. While the deal may prove to be beneficial for local vendors and consumers, it is necessary to ensure that there are other platforms in the market who can compete with the large market shares that Facebook and Jio possess.

Stronger data protection laws are required to ensure that dominant platforms make arrangements for protection of consumer data and do not collect or share data among themselves beyond the level that is required for the fulfillment of the lawful purpose. Vigilance on the privacy policies and collection of data by Jio and Facebook can also be exercised by CCPA to ensure that consumers are given effective choice and negotiation powers under the terms and conditions for the usage of these dominant platforms to decide how much of their data they want to share.

PROTECTION OF CONSUMERS OF EDUCATION: A CRITICAL ANALYSIS

[*]Sahaja Burde & [**]Arya Wakdikar

ABSTRACT

The landscape of Indian education has transformed owing to rapid expansion in the network of educational institutions. It has witnessed expeditious privatization with rampant consumerism revolving around students. India's new consumer protection regime came into effect in July 2020 with the objective of providing increased protection to consumers. However, the scope of this protection is not extended to the education sphere. The absence of an explicit mention of education as a service under the Consumer Protection Act, 1986 had led to a plethora of contradicting judgements by the Apex Court. Correspondingly, the new regime fails to address this grey-area in law. Recently, in the case of Manu Solanki v. *Vinayaka Mission University, the National Consumer Dispute Resolution Commission passed a deadlock breaking judgement. While distinguishing coaching centers from all other regular educational institutions, it held that educational institutions like colleges and universities do not provide 'services', and hence, students do not qualify as consumers. This article aims to critically evaluate the viability of this judgement by way of analyzing the propriety in exclusion of education from the definition of 'service' in the Consumer Protection Act, 2019. Additionally, the authors will compare the existing stance of students as consumers in international fora.*

I. INTRODUCTION

With the changing concept of education in the country, the Indian education system has significantly evolved in order to adapt. Education, once compared to a charitable activity[1], is now one of the major service sectors in the country. Owing to rising awareness regarding the significance of education, rapid growth in both the formal education sector and informal education sector viz. coaching centers, vocational institutions, and

[*] 4th Year, B.A. LL.B (Hons.), Indian Law Society's Law College, Pune, Maharashtra.
[**] 4th Year, B.A. LL.B (Hons.), Indian Law Society's Law College, Pune, Maharashtra.
[1] Unni Krishnan. v. State of Andhra Pradesh, 1993 AIR 2178.

pre-school, has been noted.[2] This development seeks necessary regulation of the sector, even in the province of consumer protection. The Consumer Protection Act, 1986 ("**COPRA, 1986**") lacked the mention of the term 'education' in the definition of 'service', leading to diverging views being taken by courts with regard to the applicability of CPA, 1986 to educational activities. India's recent consumer protection regime – Consumer Protection Act, 2019 ("**COPRA, 2019**") - was drafted to accommodate the changing realm of commerce in order to attain the objective of the legislature to its fullest. However, even the new regime failed to explicitly include 'education' within 'services'.

The Apex Court in 2012, in the case of *P.T. Koshy* v. *Ellen Charitable Trust*[3], passed a short order excluding education from the purview of COPRA, 1986 on the sole reason of education not being a commodity. It relied on *Maharshi Dayanand University* v. *Surjeet Kaur*[4] for the reasoning provided. In 2015, the Apex Court, in *P. Sreenivasulu.* v. *P. J. Alexander*[5] passed a contradicting judgement and held that educational activities were included within the definition of service and for this purpose relied on *Buddhist Mission Dental College & Hospital* v. *Bhupesh Khurana.*[6] In a recent case of *Manu Solanki* v. *Vinayaka Mission University* ("**Manu Solanki case**"),[7] the National Consumer Dispute Resolution Commission ("**NCDRC**") held that education did not qualify as a service under COPRA, 1986. Several judgements of the Supreme Court were analyzed to arrive at this deadlock breaking judgement. The Supreme Court has admitted the appeal filed by the complainant in the case and will decide if students qualify as consumers and if education is a service.[8]

The paper aims to analyze those Supreme Court decisions that involved the interpretation of the definition of 'service' and excluded education

---

[2] Indian Brand Equity Foundation, *Education Sector in India,* available at https://www.ibef.org/download/education-report-291012.pdf, last seen on 15/11/2020.
[3] P. T. Koshy v. Ellen Charitable Trust, 2010 (3) CPC 615 (SC).
[4] Maharshi Dayanand University v. Surjeet Kaur, 2010 (11) SCC 159.
[5] P. Sreenivasulu v. P. J. Alexander, Civil Appeal Nos. 7003-7004/2015 (SC).
[6] Buddhist Mission Dental College & Hospital v. Bhupesh Khurana, (2009) 4 SCC 473.
[7] Manu Solanki v. Vinayaka Mission University, 2020 SCC OnLine NCDRC 7.
[8] PTI*, SC to examine if educational institutions, varsities fall under consumer law,* The Hindu (21/05/2020), available at https://www.thehindu.com/news/national/sc-to-examine-if-educational-institutions-varsities-fall-under-consumer-law/article32907722.ece, last seen on 15/11/2020.

from its purview. Further, counter-arguments shall be provided in order to establish the correctness in including education within the purview of COPRA, 2019. By doing so, the paper aims to test the aptness of the judgement in the *Manu Solanki*[9] case. Further, the paper provides a study of the legal stance with regard to education as a service in the international fora in order to strengthen the argument.

II. INCLUSION OF EDUCATION UNDER CONSUMER PROTECTION

The Apex Court has in several of its judgements decided on the exclusion of educational activities from consumer protection. While doing so, it relied on different arguments that have been countered below in order to illustrate the inclusivity of education within the scope of COPRA, 2019.

1. Definition of 'Service'

For the purposes of CPA, 2019, 'service' means

> service of any description which is made available to potential users and includes, but not limited to, the provision of facilities in connection with banking, financing, insurance, transport, processing, supply of electrical or other energy, telecom, boarding or lodging or both, housing construction, entertainment, amusement or the purveying of news or other information, but does not include the rendering of any service free of charge or under a contract of personal service.[10]

1.1 Inclusion Clause

The definition can be viewed in three major parts, namely, the main part, the inclusion clause, and the exclusion clause.[11] The divergent views in question are a result of 'education' not being explicitly mentioned in the inclusion cause of the definition. However, it is pertinent to note that the definition is illustrative and not exhaustive. The mere lack of mention in the inclusion clause does not result in educational activities falling within the subsequent exclusion clause. Additionally, the usage of terms 'any' and 'potential' in the main part of the definition signifies the wide scope of the

[9] Supra 7.
[10] S. 2 (42), Consumer Protection Act, 2019.
[11] Lucknow Development Authority v. M.K. Gupta, 1994 SCC (1) 243.

definition. While 'any' might mean all or some or every, 'potential' covers all users capable of using a service in addition to existing users.[12] Hence, educational activities, fulfilling the requisites of a service i.e., provided in exchange for a consideration, fall within the main part of the definition, even in the case of it being absent in the inclusionary clause of the definition.

1.2 Exclusion Clause

The Supreme Court in *Bihar School Examination Board* v. *Suresh Prasad Sinha*[13] ("**Bihar School Examination Board**") stated that the examination fee is a payment for availing the privilege of participating in examinations and not a consideration for any service provided by the educational institute. Hence, it places educational activities in the exclusion clause of the definition owing to the absence of consideration. Nonetheless, the court acknowledges that a deficiency may occur when carrying on activities in relation to examinations but states that such deficiencies solely would not mean that the Board is a 'service-provider'. The court, however, does not provide any reasoning for this conclusion. Also, the court did not take into account an earlier judgement of the court in the case of *Buddhist Mission Dental College,*[14] where the court, while upholding NCDRC's judgment, had observed that-

> Imparting of education by an educational institution for consideration falls within the ambit of 'service' as defined in the Consumer Protection Act. Fees are paid for services to be rendered by way of imparting education by the educational institutions. If there is no rendering of service, question of payment of fee would not arise.

The mere treatment of fees as payment to avail certain privileges does not disqualify it from being a consideration for the service provided by the educational institutions to its students. In addition to availing participation in an examination, the fee paid by students is a consideration for the service of assessing answer-sheets, furnishing scoresheets, etc. For instance, the payment of re-evaluation fee by students is a consideration paid to the

[12] Ibid.
[13] Bihar School Examination Board v. Suresh Prasad Sinha, (2009) 8 SCC 483.
[14] Supra 6.

educational institute in return for their service of re-assessing answer-sheets. Additionally, the fees paid for various other facilities provided by an educational institution like library fees, hostel fees, etc., are also a consideration for the service provided in the form of infrastructure, hosting of extra-curricular activities, residential facilities, etc. Hence, placing education in the exclusion clause of the definition is the result of wrongly deducing the disqualification of fees as consideration.

2. Non-Applicability to Statutory Bodies

In addition to the finding of the Supreme Court with respect to fees as consideration, another major holding of the court in the *Bihar School Examination Board* case was exempting statutory bodies from the purview of COPRA, 1986. The Board is said to be only discharging its statutory function and not providing any service.[15] The same finding has been relied on by the court in *Maharshi Dayanand University*[16] case. Since no explicit provision in COPRA, 1986 and COPRA, 2019 exempts statutory bodies from the scope of the Act, this conclusion appears erroneous. The Supreme Court in *Lucknow Development Authority* case,[17] rightly observed that *"in the absence of any indication, express or implied there is no reason to hold that authorities created by statute are beyond the purview of the Act"*. The Supreme Court found this observation to be unfitting to the facts of the *Bihar School Examination Board* case for the sole reason that they dealt with different industries– while the former dealt with housing construction, the latter dealt with education. Although a difference in facts existed, the observation made in the *Lucknow Development Authority* case was with regard to the distinction between private and statutory bodies under CPA, 1986 generally, which stands relevant irrespective of the industry in deliberation in the case.

The exclusion of statutory bodies is tackled as a larger issue taking into consideration all public authorities under various enactments. The objective of COPRA, 2019 is the protection of consumers against services

[15] Supra 11.
[16] Supra 4.
[17] Supra 11.

provided by both private and statutory bodies. It is important to analyze the nature of the function performed to determine if it is a service and not if the body against whom a complaint is filed is a private or a statutory body. Excluding statutory bodies and the services provided by them from the provisions of COPRA, 2019 would mean to go against the spirit of the Act itself.[18]

3. Legislative Intent

In the case of *Bihar School Examination Board,*[19] the court was of the view that the objective of the Act is to cover commercial activities and that it did not intend to cover the discharge of statutory functions (relating to the conduct of examinations). It is reasonable to foresee the probable argument of the absence of legislative intent in including education in the definition of service owing to the fact that the newly drafted COPRA, 2019 fails to include the term even though there exists a gray area. However, the absence of a positive mention of the term cannot be equated to its exclusion. The rule of *expressio unius est exclusio alterius,* which literally translates to 'express mention of one thing implies exclusion of another', is regarded as a valuable servant but a dangerous master to follow in the construction of statutes and documents. The rule does not have a universal application and may be limitedly applied only when it does not lead to inconsistency or injustice. In the case of a statute revealing that the legislators did not clearly intend that the express mention of one operates to exclude all others, this rule ought not to be applied.[20]

The definition of 'service' has been discussed earlier and the wide scope of it has been established. There exists no conclusive evidence to prove the legislative intent of excluding education from the purview of COPRA, 2019. It is the objective of the Act to protect the interests of consumers[21] and the phrase 'includes, but not limited to' in the definition of service may be accrued as a way to keep the option of expansion of such protection to various sectors and consumers open. With the changing notion of

[18] Ibid.
[19] Supra 12.
[20] Union of India v. B. C. Nawn, (1972) 84 ITR 526 Cal.
[21] Supra 10, Preamble.

education in the country and the exposure of risk to student consumers, as identified in cases, in the form of deficient services, it is appropriate to include education in the ambit of CPA, 2019 as it fulfils all essentials of a service.

4. Non-commercialized Activity

Another argument resorted to by the courts to exclude education from the definition of service is that education in India lacks the feature of commercialism. Courts have opined that education has never taken the shape of commerce in the country and cannot be treated as a trade or business. Imparting education has always been a religious duty and a charitable activity in the country,[22] thereby, leading to exclusion of students from the definition of consumers even if they pay fees.

The view taken by courts can safely be said to be obsolete considering the eminent advertising of educational institutions in order to sell a seat to students who are treated no differently than consumers. Nonetheless, the definition of service under COPRA, 2019 does not require a profit-making motive as an essential for any activity to fall within the scope of the definition but only excludes service rendered free of charge. However, presence of consideration i.e., imparting of education for a fee has already been established. The absence of a profit-making motive is no bar to education being an industry. Even the contention that "*education is a mission or a vocation*" and not a commercial enterprise, does not rule out the possibility of it being classified as an industry if it possesses industrial attributes.[23]

The education industry has been going through rapid strides of commercialization, especially, as a result of privatization. The emphasis on education has led to increased students opting for higher education in the country, and this need is majorly catered to by private institutions in the country. Increased autonomy given to private institutions has led to issues

[22] Supra 1.
[23] Bangalore Water Supply & Sewerage Board v. A. Rajappa, (1978) 2 SCC 213.

such as higher fee structure, capitation fee, false representation, etc.[24] Courts have addressed the issue of false claims of affiliation to universities and have held such an act of misrepresentation to fall within the ambit of COPRA, 1986, amounting to 'deficiency in service'; and in such a case, students have been given protection against the services rendered by educational institutions.[25]

In the *Manu Solanki* case,[26] the most recent ruling in relation to education as a service, the NCDRC relied on all the above arguments (which have been countered) and cases in order to reason the exclusion of education institutions and their activities from the consumer protection regime. Another major finding of the Commission in the case was the distinction between educational institutions like schools and colleges and coaching centers. Coaching centers are excluded from the definition of educational institutions on the ground of non-provision of degree or diploma, thus, placing them within the scope of COPRA, 2019. Additionally, the learned counsel also contended that coaching centers, unlike regular schools, did not impart real knowledge and that they functioned with a profit-making motive, expanding through the franchise route. However, as stated above, educational institutions have also emerged as commercial enterprises, taking the franchise route, similar to that of coaching centers.

III. STUDENTS AS CONSUMERS IN THE INTERNATIONAL FORA

The treatment of education in foreign countries will help in understanding the characteristics of the activity in detail in order to determine if the inclusivity of education under COPRA, 2019 is logically sound. In an attempt to do so, the authors have discussed below the position of educational institutions under consumer law in the United Kingdom ("**UK**"), the United States of America ("**USA**"), and Australia.

1. United Kingdom

[24] N. Rathee & S. Thakran, *Commercialization of Education in India*, 2 International Journal of Multidisciplinary Research and Development (2015).
[25] Dr. Alexander Education Foundation v. Union of India, 2009 SCC Online Del 2178.
[26] Supra 7.

In the UK, the recently enacted Consumer Rights Act, 2015,[27] encompasses the rights of UK consumers, including the rights of university students. The Act construes students accessing education as purchasing a service, and are recognized in law as 'consumers', implying that students should receive the same protection as any other consumer buying goods and services. This Act rightly interprets the hybrid relationship of students and educational universities, as it espouses the principles of both private law and public law. The existence of the said relationship was first discerned by the Court of Appeal in *Clark* v. *University of Lincolnshire and Humberside,*[28] which dealt with the matter of regulation of education.

Universities providing Higher Education in the UK have to comply with the consumer protection law and meet certain standards set by the Competition and Markets Authority ("**CMA**").[29] CMA aids in advising higher education and further education institutions, with respect to their responsibilities under consumer law. CMA lays emphasis on the education sector's need to provide clear and transparent information that helps students to make informed decisions about where to study and stresses on having a fair and balanced terms and conditions that provide a clear contractual relationship between a student and their university, and robust, accessible and clear complaint handling process that allows students to hold universities accountable.

CMA published a guide for UK higher education providers, giving advice on consumer protection law, clarifying what universities should do in core areas such as information provision to current and prospective students, terms and conditions, and complaint processes and practices.[30] In the CMA's view, the time and investment that students commit to their studies are quite substantial, and thus should be safeguarded from any kind of potential disruption, since students are in a weaker position than the

[27] Consumer Rights Act, 2015 (United Kingdom).
[28] Clark v. University of Lincolnshire and Humberside, [2000] 3 All ER 752.
[29] *Consumer Protection: Detailed Information*, Government of United Kingdom, available at https://www.gov.uk/topic/competition/consumer-protection, last seen on 14/12/2020.
[30] *Undergraduate Students: Your Rights under Consumer Law*, Competition & Markets Authority, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415732/Undergraduate_students_-_your_rights_under_consumer_law.pdf, last seen on 15/11/2020.

universities. The authority ensures that these universities achieve the required standard, in order to provide students with the best of facilities. Alongside the 2015 legislation, the CMA guidance system encompasses certain primary consumer rights legislations, mentioned as follows:

1. Consumer Protection from Unfair Trading Regulations, 2008[31] ("**CPRS**"): In brief, this statute prevents the usage of unfair commercial practices towards consumers and applies from before a student has accepted an offer through to enrolment.

2. Consumer Contracts (Information, Cancellation and Additional Charges) Regulations, 2013[32] ("**CCRs**"): Broadly, the legislation requires universities to give students access to specific information and details before the contractual relationship is formed and to inform students of their cancellation rights if the contract is made off-premises.

3. CRA, 2015[33]: This Act is the latest addition to the regime of consumer protection. The Act facilitates a student to demand 'repeat performance' as a remedy if a contract is not being formulated with 'reasonable care and skill'. The agreement is taken to incorporate anything said to the consumer by, or in the interest of, the service provider which impacts the consumer's choice to go into the agreement. The CMA may take compliance activity against a supplier and is additionally dedicated to working with the area to improve practice. In England, compliance is presently a state of admittance to public assets and will be a necessity for section onto the higher education register under the Office for Students ("**OfS**"). These progressions occur with regards to the Higher Education and Research Bill that will support the passage of new providers and competition between institutions.

In the UK, students accessing higher education are considered as consumers availing service, i.e., education. Whereas, in India, the NCDRC

[31] Consumer Protection from Unfair Trading Regulations, 2008.
[32] Consumer Contracts (Information, Cancellation and Additional Charges) Regulations, 2013.
[33] Supra 27.

held that students do not qualify as consumers and hence students won't be protected under the consumer law. In addition to considering students as consumers, the UK's consumer protection framework is also extremely systematic and detailed leaving close to no room for universities to infringe upon the student's consumer rights. Their system is extremely well-equipped, primarily focusing on student welfare. The CMA regime is extremely efficient as it lays out information about all the higher education universities that help students in making an informed decision about their potential educational prospects. In India, owing to the advent of so many private universities it becomes imperative to adopt a similar system, in order to safeguard student's careers.

2. Australia

In Australia, the Australian Consumer Law ("**ACL**")[34] is a uniform legislation for consumer protection applying to the Commonwealth of Australia and is a law operational in all the states and territories. ACL can be found in the 2nd Schedule of the Competition and Consumer Act, 2010. It is a fairly new legislation, which replaced around 20 distinct legislations around the consumer law fora. Over time, Australia's higher education system has transformed itself into a culture of consumerism with the student at the center as the consumer[35] seeking redressal. Therefore, the current legislation defines consumers broadly as *"a person to whom goods or services are or may be supplied by participants in the industry*".[36]

The Australian legal and judicial framework has recognized some consumer protection rights do accrue to the students. The relationship between the student and Higher Education Institutions ("**HEI**") is multifaceted, overlaid by the principles of common law and under the statute. Additionally, the Unfair Contract Terms ("**UCT**") regime in the ACL protects students in the context of education from unfair terms in a contract, such as the plan and conveyance of an educational course, distinct from promotional activities. The provisions of UCT will be referred to if

[34] Australian Consumer Law, Schedule 2, Competition and Consumer Act, 2010.
[35] Stephen Corones, *Consumer Guarantees and the Supply of Educational Services by Higher Education Providers,* University of New South Wales Law Journal (2012).
[36] S. 3, Schedule 2, Competition and Consumer Act, 2010.

the services come under the scope of 'trade and commerce',[37] as defined in the ACL, it contains a new extended definition of 'trade or commerce'. The definition includes any 'business activity' or any 'professional activity' whether or not for profit. The words 'any professional activity' arguably impact the application of the ACL to providers of educational service. In the case of *Shahid* v. *Australasian College of Dermatologists,*[38] it was held that the activities of associations of professionals such as colleges were not excluded from the expression 'any professional activity'. According to the Australian framework, various educational activities that make up the supply of educational services will be characterized as carrying on a profession and will thus fall under the extended meaning of trade and commerce under the ACL.

The ACL is administered by the Australian Competition and Consumer Commission ("**ACCC**") and state and territory consumer protection agencies, and is enforced by all Australian courts and tribunals, including the courts and tribunals of the states and territories.

There is a stark difference between the Australian and Indian consumer law framework. In addition to Australia being one of the nations that extended consumer protection to its students, it also has a robust framework of laws under the UCT regime which further empowers the protection regime for students. Under the ACL, it categorically mentions 'service' under the scope of 'trade and commerce,' which is defined as a 'business activity' or any 'professional activity' whether or not for profit.

On the contrary, in India, courts have stood their ground that education does not fall under the ambit of a commercial/profit-making activity, in spite of the ever-growing privatization in the sector. India follows an era old school of thought that considers education and the imparting of education as a religious and godly act close to charity.

3. United States of America

[37] Ibid., S.2, Schedule 2.
[38] Shahid v. Australasian College of Dermatologists, (2008) 248 ALR 267.

Since 1960, the legal relationship between students and educational institutions has been multidimensional in the USA. The relationships are often fiduciary, contractual or constitutional. These relationships take the form of rights either through the Constitution or by legitimizing students as consumers and granting them protection under the consumer law. The education sector heavily contributes to the country's GDP growth.[39] The Educational Industry in the USA is classified as a service and is classified under Code 61 in the North American Industry Classification System ("**NAICS**").[40] The Educational Services sector comprises establishments that impart training in a wide variety of subjects. This particular training is provided by specialized establishments, such as colleges, universities, and training centers. These establishments may be privately owned and operated for profit or not for profit, or they may be publicly owned and operated. Additionally, the 1962 Consumer Bill of Rights asserts that consumers have the right to consumer safety, information preventing fraud and deceit, informed choice, to choose from multiple alternative options and the right to complaint, to be heard and addressed. Provisions analogous to these rights are mentioned in the Higher Education Act of 1965.[41]

There are a number of federal laws that provide protection to students with respect to the current issues that hamper students in the country, like issues of student loans and debts. In lieu of that, the Federal Trade Commission ("**FTC**") is a body that administers a wide variety of consumer protection laws, alongside other federal agencies.[42] The objective of FTC is to afford consumers a deception free marketplace and maintain competition by preventing anticompetitive business practices. FTC has administrative as well as enforcement abilities under forty-six other statutes, thirty-seven of which relate to the FTC's consumer protection framework. In addition to

[39] *Changing the lens: GDP from the industry viewpoint*, Deloitte., available at https://www2.deloitte.com/us/en/insights/economy/spotlight/economics-insights-analysis-07-2019.html, last seen on 15/11/2020.
[40] *Educational Services: NAICS 61*, U.S. Bureau Of Labor Statistics, available at https://www.bls.gov/iag/tgs/iag61.htm#:~:text=Workplace%20Trends-,About%20the%20Educational%20Services%20sector,a%20wide%20variety%20of%20subjects, last seen on 14/11/2020.
[41] Higher Education Act, 1965 (United States of America).
[42] S. 5 (a), Federal Trade Commission Act, 1914 (United States of America).

this, FTC is also the investigative and enforcement authority, it uncovers deception, unfair activities, or violation of any statute under which it has authority.[43] Upon completion of an investigation, if the FTC has a reason to believe that a violation exists, it may file a complaint at the Administrative Law Judge ("**ALJ**").

The USA educational sector comprises of establishments such as colleges, universities, and training centers that impart training in a variety of subjects. The USA's consumer protection regime adduces institutions which may be privately owned or publicly owned and operated for profit or non-profit as service providers, unlike in the Indian system wherein, only recently in the *Manu Solanki* case, a difference between regular educational institutions and coaching centers was drawn, and it was further held that coaching centers don't fall under the purview of educational institutions. The consumer protection mechanism of USA, although lacking centralization, provides in depth and variety of protection. Its strength lies in the array of governmental actors, formal legal rights, and remedies protecting consumers. Its weakness lies in the unequal reality of who has access to the government and the courts.

IV. CONCLUSION

The Indian education system, as discussed above, has been developing with time and the newly tabled National Education Policy 2020 is an indication of the same. With such introductions in the system, it is crucial that the stand with respect to educational activities such as the position of educational institutions within consumer law is crystal clear. It becomes extremely vital for the nation which is inching towards such a huge educational reform that the redressal system related to educational matters should be systematic, clear, and hassle free. This becomes even more vital when the Ministry of Education is trying to seek Ivy League institutions and other wealthy private institutions' establishments in the country.[44]

---

[43] *Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority,* Federal Trade Commission, available at https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, last seen on 15/11/2020.

[44] K. Sharma, *Ivy League curriculum to foreign faculty, Jio University's competitors also had it all*, The Print, available at https://theprint.in/india/governance/ivy-league-curriculum-to-

The authors have, by way of discussing various judicial pronouncements, determined the position of educational institutions under consumer law in the country. Evaluating legally and logically, the authors have attempted to substantially support the inclusivity of educational institutions within the definition of 'services' by countering the major arguments of the court – non-inclusion of 'education' in the definition of 'service', non-commercialization of education in India, exemption carved out for statutory bodies, and the lack of legislative intent. Countries like UK, USA, and Australia have laid emphasis on students' rights as consumers, which is clearly depicted in the laws of the countries respectively.

The privatization of the educational sector in the country requires such protection be given to student consumers in India as well, as the laws in these foreign countries are a proof to the fact that education is more than just a charitable activity and can be construed as a service. It is of utmost importance for educational activities, rendered by both private and statutory bodies to fall within the purview of consumer protection in order to guarantee effective justice, in terms of both cost and time, to students. The protection extended to student consumers must be in proportion to the emphasis laid on education in the country in order to prevent deterrence of students from education.

foreign-faculty-jio-universitys-competitors-also-had-it-all/116109/, last seen on 14/12/2020.

COOPERATIVE FEDERALISM VIS-À-VIS ESTABLISHMENT OF AUTHORITIES UNDER CONSUMER PROTECTION ACT, 2019

[*]Rahul Rishi, [**]Puja Saha & [***]Sonakshi Singh

ABSTRACT

"Federalism isn't about protecting States' rights. It's about dividing power to better protect individual liberty."

- Elizabeth Price Foley

India takes pride in the democratic structure of the country. However, democracy is effective only when it is shaped in a federal way, where the power to govern is shared between the Centre and the States. It ensures that the voices of all the parties are heard, whether they are in majority or minority. Cooperative federalism is not a modern concept but has been in use since ancient times. It is a concept in furtherance of social justice and equality as enshrined in the Constitution of India. Where on one side, the institution of democracy advocates majority opinion, federalism on the other side, ensures that the minority opinion is also adjusted with the former, giving effect to social justice. Redistribution of powers from the Centre to States and consecutively to Panchayats and local bodies facilitates to further the principles of Constitution, namely unity, social justice and democracy. This leads to the harmonious operation of the whole system.

Maintaining strong Centre-State relations is the key to national development. Coordination and cooperation between the Centre, States and local bodies must be ensured at each and every sphere of governance. Establishment of authorities and allied powers of bodies at state and national level must be undertaken with the participation of both levels of governments. This is a requisite for representation of the diverse interests of the population of a country like India.

In this article, the authors seek to study the provisions of the Consumer Protection Act, 2019 ("CPA") with respect to the establishment of authorities in light of the Constitutional principle of cooperative federalism. In this paper, the authors have firstly

[*] Rahul Rishi, Lawyer, Nishith Desai Associates, New Delhi.
[**] Puja Saha, Lawyer, Nishith Desai Associates, New Delhi.
[***] Sonakshi Singh, V Year Student, Amity Law School, Noida.

studied the concept of cooperative federalism in India. Secondly, the provisions of the aforesaid CPA which are in conflict with the concept of cooperative federalism, have been analyzed. Lastly, the authors in the conclusion discuss the importance of co-operative federalism and raise certain important questions in terms of the distribution of powers between the Centre and the State.

I. CONCEPT OF CO-OPERATIVE FEDERALISM IN INDIA

Federalism is one of the salient features of the Constitution of India (**"Constitution"**). While, the term 'federalism' itself is nowhere directly mentioned in the Constitution, there are several provisions in the Constitution that indirectly connote the existence of a federal character of the structure of Government in India. The multi-cultural, multi-religious and multi-lingual nature of the country justifies the federal character of the governmental structure in order to represent the interest of the diverse population of the nation.

Article 1[1] of the Constitution describes India as a 'Union of States'. This shows that India is not completely federal in nature but can be said to be 'quasi-federal' or 'semi-federal' or 'a federation with strong unitary features'. In order to balance the diverse interest, it is essential that there is coordination between the Centre and the States. Therefore, the concept of cooperative federalism bears immense importance for good governance of the State. Strong Centre is the essence of cooperative federalism as it ensures the strength of the states.

Cooperative federalism means a combination of cooperation and inter-dependence between the Centre and the States to ensure smooth governance of the country. This is effective in maintaining cordial relations within the diverse population of the country and ensuring that such interests do not clash with each other. Within the state also, cooperative federalism requires the coordination between the State Governments and other Local Government bodies like panchayats, municipal corporations, etc. Such cooperation is required to give all governmental bodies a broader national market and natural resources and provide a national platform for

[1] Art. 1, the Constitution of India.

human capital to bring prosperity to the nation as a whole. The existence of such cordial relations is evident through the Constitutional provisions enshrined in the Preamble, Directive Principles of State Policy and through the establishment of bodies like the Inter-State Council (Article 263[2]), National Development Council, Zonal Councils (7th Constitutional Amendment), Finance Commission, Planning Commission and like bodies. The Zonal Councils divided the country into five zones for better governance and representation of varied interests. The Constitution enlists the legislative and taxation powers of the Central and State Governments through division into three lists – Union list, State list and Concurrent List.[3]

The concept of cooperative federalism grew in significance in the 1990s when the coalition government was formed in the Centre with the national and regional parties. However, in the recent years, the power has shifted more towards the Centre and created an imbalance in the cooperative nature of Union-State relations.

1. Punchhi Commission

The Punchhi Commission on Centre-State relations in its report[4] observed that there has been a tilt in the distribution of legislative, administrative and financial powers in favor of the Centre. It stated that while in matters of security it is justified for Centre to bear more powers, in other matters such as development, the Centre must respect the autonomy of the State and Local Governments. In such matters, the Centre's role must be limited to framing broad policies, allocating funds and coordination while giving the States and Local bodies the autonomy of implementing. There are several instances of conflicts between the lists where the powers of Centre and State both extend. Such conflicts are resolved by applying the doctrine of repugnancy under Article 254(1)[5] of the Constitution. There are numerous

[2] Ibid, Art. 263.
[3] A. S. Reddy, *Union state relations in India need for cooperative federalism a selective study*, Sri Krishnadevaraya University, available at https://shodhganga.inflibnet.ac.in/handle/10603/86844, last seen on 14/09/2020.
[4] The Commission on Centre-State Relations*, Volume-II: Constitutional Governance and The Management of Centre-State Relations,* available at http://interstatecouncil.nic.in/wp-content/uploads/2015/06/volume2.pdf, last seen on 14/09/2020.
[5] Supra 1, Art. 254 (1).

instances where the Centre has encroached upon the powers of States, education being one area. No state has the authority to make any law which is inconsistent with All India Council for Technical Education Act, 1987, which is the central legislation. This shows how the Centre is increasingly becoming dominant in governance. Executive coordinative federalism is ensured through inter-governmental delegation of powers (Articles 258[6], 258A[7] of the Constitution), directives given to the States by the Centre (Articles 256[8], 257[9] of the Constitution), All India Services (Article 312[10] of the Constitution) and Inter-State Council (Article 263[11] of the Constitution). The Commission recommended that in matters of List-III, the Centre and States must reach some agreement. Further, it was recommended that in case of emergency, provisions under Articles 352[12] and 356[13] of the Constitution should be used only as a 'last resort' and a proper independent statute must be framed for governing the legal framework. This was suggested in light of the stringent limitations imposed on State autonomy under aforesaid articles, besides curtailing the freedom of the people. Therefore, an independent legal framework would be preferable to tackle situations wherein Central intervention is required but strict boundaries of Articles 352 and 356 are not essential. Lastly, the Commission has suggested for maintaining the balance of powers between the Centre and States in order to eliminate the increasing dominance of the Centre.

2. Judicial Stance

The Apex Court had interpreted the federal nature of India in the case of *S.R Bommai* v. *Union of India*[14], wherein it said that "*the essence of a federation is the existence of the Union and the States and the distribution of powers between them. Federalism, therefore, essentially implies demarcation of powers in a federal compact*".

[6] Ibid, Art. 258.
[7] Ibid, Art. 258A.
[8] Ibid, Art. 256.
[9] Ibid, Art. 257.
[10] Ibid, Art. 312.
[11] Supra 2.
[12] Ibid, Art. 352.
[13] Ibid, Art. 356.
[14] S. R. Bommai v. Union of India, (1994) 3 SCC 1.

Further, the Court went on to say that "*Democracy and federalism are the essential features of our Constitution and are part of its basic structure*".[15] While the Apex Court did not specifically make use of the term 'cooperative federalism' in this case, it indirectly upheld its spirit by saying that:

> Federalism implies mutuality and common purpose for the aforesaid process of change with continuity between the Centre and the States which are the structural units operating on balancing wheel of concurrence and promises to resolve problems and promote social, economic and cultural advancement of its people and to create fraternity among the people.[16] The division of power between the Union and the States is made in such a way that whatever has been the power distributed, legislative and executive, be exercised by the respective units making each a sovereign in its sphere and the rule of law requires that there should be a responsible Government.[17]

The Supreme Court of India has interpreted the concept of cooperative federalism in recent cases as well. In *Jindal Stainless Steel* v. *State of Haryana*,[18] the Apex Court reiterated the principles of cooperative federalism in India by saying that

> the Union and the States are coequal in the Indian federal structure. Our framers created a unique federal structure which cannot be abridged in a sentence or two. The nature of our federalism can only be studied having a thorough understanding of all the provisions of the Constitution.[19]

Further, the Supreme Court in *Swaraj Abhiyan* v. *Union of India*[20] stated that:

> The principle of federalism as present in India cannot be explained in a sentence or two; rather a detailed study of the each and every provision of the Constitution would inevitably point that India has divided sovereignty in the form of Centre on one hand and States on the other. Each power house is independent in its own terms. The constitutional scheme invariably leads to the conclusion that at times these institutions meet and interact at various levels to achieve the cherished constitutional goal of cooperative federalism.[21]

[15] Ibid.
[16] Ibid, at paragraph 165.
[17] Ibid, at paragraph 169.
[18] Jindal Stainless Steel v. State of Haryana, AIR 2016 SC 5617.
[19] Ibid, at paragraph 185.
[20] Swaraj Abhiyan v. Union of India, (2018) 12 SCC 170.
[21] Ibid, at paragraph 84.

The most recent case of *Government of NCT of Delhi* v. *Union of India*,[22] also known as 'Special status of Delhi case' has also thrown light upon the concept of cooperative federalism, wherein the court took note of its own following observation in the case of *NDMC* v. *State of Punjab*:[23]

> The constitutional vision beckons both the Central and the State Governments alike with the aim to have a holistic edifice. Thus, the Union and the State Governments must embrace a collaborative federal architecture by displaying harmonious coexistence and interdependence so as to avoid any possible constitutional discord. Acceptance of pragmatic federalism and achieving federal balance has become a necessity requiring disciplined wisdom on the part of the Union and the State Governments by demonstrating a pragmatic orientation. The Constitution has mandated a federal balance wherein independence of a certain required degree is assured to the State Governments. As opposed to centralism, a balanced federal structure mandates that the Union does not usurp all powers and the States enjoy freedom without any unsolicited interference from the Central Government with respect to matters which exclusively fall within their domain.[24]

From the above-mentioned observations of the Apex Court over the years, it can be seen that the highest tier of the judiciary has stressed upon the importance of cooperation between the Centre and States owing to the federal character of governance. It has upheld the spirit of cooperative federalism by using different terms like 'collaborative' or 'pragmatic' or 'coequal' and other like terms, but whose interpretation would reveal the same concept.

3. Position in the United States of America

In the United States ("**U.S.**"), cooperative federalism has been justified through Constitutional principles. They are threefold: the liberal interpretation of Supremacy clause given under Article VI, Clause 2[25] of the Constitution of the U.S.; the contention that the Necessary and Proper Clause given under Article 1, Section 8[26] ('Elastic Clause') empowers the Federal Government to make required laws in carrying out its inherent

[22] Government of NCT of Delhi v. Union of India, (2018) 8 SCC 501.
[23] NDMC v. State of Punjab, (1997) 7 SCC 339.
[24] Government of NCT of Delhi v. Union of India, (2018) 8 SCC 501.
[25] U.S. Constitution, Article VI, Cl. 2.
[26] Ibid, Article I, S. 8.

powers; and the narrow interpretation of the Tenth Amendment-which limits the powers of the Federal Government to only those granted to it by the Constitution and grants the States all other powers not expressly prohibited from delegation to the States by the Constitution.

II. CO-OPERATIVE FEDERALISM VIS-À-VIS APPOINTMENT OF MEMBERS OF THE STATE AND DISTRICT COMMISSION UNDER THE CONSUMER PROTECTION ACT, 2019

The provisions relating to the appointment of members of the District and State Commission in the Consumer Protection Act, 2019 ("**CPA**") are in conflict with the Constitutional principle of cooperative federalism. These provisions clearly show dominance in status of Central Government in comparison to the State Governments, while the principle of cooperative federalism requires both the levels of Government to function in cooperation with each other, most of these provisions relate to the power of establishment of authorities under the CPA. These provisions are discussed below.

1. Cooperative federalism under the Consumer Protection Act, 1986

As stated earlier, cooperative federalism requires cooperation and inter-dependance between the Centre and the State, which acts as a method of check and balance to prevent the accumulation of excess power at the Centre.[27] In the erstwhile Consumer Protection Act, 1986 ("**CPA, 1986**"), the principle of cooperative federalism was more coherent than it is in the new CPA.

The establishment of District Forums and State Commission under the erstwhile CPA, 1986 gave more autonomy to the States. The District Forum earlier constituted of a person who is or qualified to be a District Judge as its President. The other two members were appointed by the State Government on the recommendation of the Selection Committee, which

[27] M. Tully, *India's far from cooperative federalism*, Hindustan Times, available at https://www.hindustantimes.com/columns/india-s-far-from-cooperative-federalism/story-teUUoRnjTzsABfyix0y7JL.html, last seen on 08/02/2021.

constituted of the President of the District Forum as its Chairman, the Secretary of Law Department of the State and the Secretary of Department dealing with Consumer Affairs.[28] The composition the State Commission had a person who is or previously was a High Court Judge as its President, who was to be appointed by the State Government, in consultation with the Chief Justice of that High Court.[29] The other members were appointed on the basis of the recommendation of the Selection Committee by the State Government. Such selection committee had the same members as a District Forum, except that the President of State Commission acted as its Chairman.[30] The appointment of members of the National Commission was done by like authorities in the Central Government. Therefore, it can be seen that the power of appointment of authorities under the erstwhile Act was distributed evenly between the Centre and the States, wherein each had autonomy in its own sphere, giving effect to the principle of cooperative federalism in the sense interpreted by the judiciary in India. As the judicial stance stresses upon the balance of powers between the Centre and the States and abstaining the Centre from indulging in unsolicited interference with the powers of the State, the erstwhile CPA, 1986 had upheld this spirit of the principle of cooperative federalism in its true sense.

2. The Present Scenario

While as per the CPA, 1986, the State Government had the power to appoint members of the District and the State Commissions, as these were the retired judges of the High Court, now, as per the new Act, the State Government can appoint these members only 'in consultation with' the Central Government, as specified under Section 28(2).[31] The Consumer Protection (Qualification for appointment, method of recruitment, procedure of appointment, term of office, resignation and removal of the President and members of the State Commission and District Commission) Rules, 2019, lay down the qualifications for the appointment of the President and other members of the District Commission. As per

[28] S. 10, the Consumer Protection Act, 1986. (stands repealed)
[29] Ibid, S. 16.
[30] Ibid.
[31] S. 28 (2) of the Consumer Protection Act, 2019.

the aforesaid rules, a District Judge or a person eligible to become a District Judge only, can be appointed as President of the Commission. It is to be noted here that a District Judge is appointed by the Governor of a State, in consultation with the High Court, as per Article 233[32]. Therefore, it is difficult to comprehend as to why the Central Government would intrude upon the State's power to appoint members of the District Commission, if the former has no role to play in the appointment of District Judges. Such central intervention curtails the autonomy of the states and over-centralizes this domain. This goes against the spirit of cooperative federalism which requires a combination of individual autonomy and cooperation of each level.

Besides the Central intervention in the appointment of the aforementioned authorities, the Central Government is further empowered to alter the pecuniary jurisdiction of the District and State Commissions under the new CPA. The Act does not involve any role of or consultation with the concerned State before taking such decisions. This, again, is an act of over-centralization.

III. CONCLUSION

Given the desired constitutional principle of spirit of mutuality between the Centre and States, it is important to understand that co-operative federalism is often a function of the Government's electoral strength in the Parliament. One must understand the nuances of co-operative federalism through a dispassionate analysis of the effects of electoral majorities by ruling dispensations in the Parliament. Thus, one needs to ask whether India is moving away from coalition politics to a majoritarian electoral politics where the tenets of co-operative federalism are shifting more towards coercive federalism. Are we reconciling conflicts between the Centre and States or are we trying to achieve a single political union despite multiple administrative and governance peculiarities?

How do we ensure that constitutionally allocated distribution of powers between one or more levels of Government are fine-balanced? Do we

[32] Supra 1, Art. 233.

strengthen the Constitution or do we strengthen electoral institutions to ensure that our electoral processes do not reflect a dominant party federalism? Will regional assertions despite a strong Centre provide the answer or will regionalization be subsumed into federalization in the name of national unity?

What we must keep in mind is that whenever there is a rise of centralizing tendencies through an electoral process, there is invariably an encroaching of regional autonomy, and resultantly conflictual relation between Centre and States in relation to enforcement of issues falling under the concurrent list.

THE LEGAL COMPLIANCES OF E-COMMERCE ENTITIES UNDER THE CONSUMER PROTECTION ACT, 2019

[*] *Shivani Dutta*

ABSTRACT

This paper attempts to analyze the Consumer Protection (E-Commerce) Rules, 2020 as enumerated by the Central Government to regulate the transactions in the digital market in India. With the wider application of the Consumer Protection Act, 2019 ("CPA, 2019") to all goods or services bought or sold over the digital or electronic network, including digital products; marketplace e-commerce entities and inventory e-commerce entities; all e-commerce retail and unfair trade practices which falls within the definition as defined under the CPA, 2019 across all models of e-commerce, it is pertinent to discuss about the redressal mechanism which shall be available to a consumer in case his rights are violated. The Rules in addition to the duties and liabilities as seller, makes it mandatory for the foreign entities who carry on business in India through digital platforms, to appoint an Indian resident as a nodal person to ensure compliance with the CPA, 2019. Non-compliance with the rules will attract liability under the CPA, 2019 which may also result in fines or imprisonment. However, the question which needs to be answered is how far the redressal agencies under the CPA, 2019 can bring within its jurisdiction the foreign e-commerce entities. Will the nodal officer be vicariously responsible? Can they compel them to go for mediation? Thus, in this paper, the above-mentioned questions shall be discussed in length.

I. INTRODUCTION

The business of e-commerce is not a new phenomenon anymore. It has reached its zenith in India. The shift from traditional brick and mortar to the online purchase of goods and availing of services has opened the market so wide that it becomes difficult to trace the boundary to which it

[*] Shivani Dutta, Research Scholar, National Law School of India University, Bangalore. She was assisted by Mr. Nishant Nagori, II Year Student, Rajiv Gandhi National University of Law, Punjab. He has been credited as a co-author of this article by the author.

extends. The easy accessibility and the change in lifestyle of the people, coupled with the various offers available on online platforms inclines them to opt for the online purchase[1] of goods as well as to avail services. Thus, it is of utmost necessity that there needs to be in place certain regulatory frameworks so that the consumers do not find themselves in a helpless situation when any grievance creeps up. The consumers have the right to be protected against fraudulent, misleading or deceitful information and any other circumstances in which the consumer has to make an informed choice. The objective of consumer protection legislation is to prohibit unfair trade practices; to inform the consumers about quality, quantity, potency, price of the goods and services; to educate and to redress the consumers in case there is any defect in the goods or deficiency of services. These rights also extend to e-commerce transactions according to the Consumer Protection Act, 2019[2] ("**CPA, 2019**") which has brought within its ambit e-commerce entities including foreign entities. E-commerce according to the CPA, 2019 means buying or selling of goods or services including digital products over a digital or electronic network.[3] One of the challenges over sale of goods or services over electronic network is the territorial jurisdiction issue, where one cannot easily identify the place of contract or the jurisdiction where the contract was completed. With the acceptance of the terms and conditions in e-commerce transactions the buyer basically subjects oneself to the clauses of the seller without getting an opportunity to negotiate the terms. In such a situation when the goods received are defective or if there is any deficiency of service, the right to redressal of the consumers shall not be affected. The Consumer Protection Act, 1986 ("**CPA, 1986**") failed to deal with those complexities which arose in the digital market. Thus, with the enactment of the 2019 Act, an attempt has been made to fill those gaps and protect the consumers in the digital platform. To provide a comprehensive legal framework to regulate the marketing, sale and purchase of goods and services online, the Ministry of

[1] D.K. Rigby, *The future of Shopping*, Harvard Business Review, available at https://hbr.org/2011/12/the-future-of-shopping, last seen on 24/12/2020.
[2] It has replaced the Consumer Protection Act, 1986 and was enacted on 9th August, 2019.
[3] S. 2 (16), Consumer Protection Act, 2019.

Consumer Affairs, Food and Public Distribution has framed the Consumer Protection (E-commerce) Rules, 2020 ("**E-Commerce Rules**"). The E-Commerce Rules exhaustively deal with certain procedural requirements which need to be complied with by the e-commerce entities before offering goods and services in India. The violation of the Rules by any e-commerce entity, including a foreign entity, is liable for punishment as per the provisions of the CPA, 2019.[4] In addition to the 2019 Act and the E-Commerce Rules, the entities who are engaged in e-commerce are also governed by numerous other regulations such as the Legal Metrology Packaged Commodities (Amendment) Rules, 2017, which requires all e-commerce entities to display certain information on their websites; The Foreign Exchange Management (Non-Debt Instrument) Rules, 2019 which places specific conditions on marketplace entities with foreign direct investment; The Information Technology Act, 2000 which applies to electronic transactions and communications, and the Information Technology (Intermediaries Guidelines) Rules, 2011 which regulates intermediaries.[5] However, the scope of this paper is limited only to the CPA, 2019, including the E-Commerce Rules which govern e-commerce entities and to look into whether the redressal agencies established under the CPA, 2019 can summon the foreign entities to its jurisdiction.

II. E-COMMERCE UNDER THE CONSUMERS PROTECTION ACT, 1986

Prior to the enactment of the CPA, 1986, the rights of consumers were scattered in various legislations in India. A comprehensive legislation on consumer protection in India was enacted in line with the United Nations Guidelines on Consumer Protection[6] in 1986. With technological advancement, the E-Commerce market reached its own zenith, however there was no specific legislation to govern the E-Commerce entities in

[4] Supra 3, Ss. 88, 89, 90 and 91.
[5] *India: Consumer Protection (E-Commerce) Rules, 2020*, Mondaq, available at https://www.mondaq.com/india/dodd-frank-consumer-protection-act/980140/consumer-protection-e-commerce-rules-2020, last seen on 24/12/2020.
[6] U.N. General Assembly, *United Nations Guidelines for Consumer Protection,* Res. 39/248, Sess. 39, U.N. Document A/RES/39/248, available at https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf, last seen on 24/12/2020.

India. Under the CPA, 1986 complaints against online transactions were brought under the provisions of 'deficiency in service' under S. 2(1)(g) or 'unfair trade practices' under S. 2(1)(r) of the Act. Some of the major challenge(s) in electronic transactions is lack of transparency as to the parties to the contract, the place of jurisdiction, greater risk of fraud, problems relating to delivery, return of goods etc.

Some of the decisions of the consumer courts with respect to online transactions are reproduced herein. In the case of *Rediff.com India Ltd.* v. *Urmil Munjal*[7], there was no Return Policy mentioned in the online portal; where the consumer on being dissatisfied with the product wanted to return, it was considered to be a 'deficiency of service' by the consumer court.

In one case, the consumer court could not reach to a concrete decision when an online transaction involved different jurisdictional areas.[8]

III. E-COMMERCE UNDER THE CONSUMER PROTECTION ACT, 2019

As discussed above, the CPA, 1986 failed to protect Indian consumers in the e-commerce market, which compelled the Government of India to enact a legislation to protect the 21st century consumers in the era of globalization. To unfold the discussion on the changes pertaining to the governance of E-Commerce under the CPA, 2019 it is important to look into some of the important definitions which has been explicitly inserted in the CPA, 2019 and analysis about the feasibility of its implementation.

(i) E-consumer: One of the drastic changes which has been brought under the CPA, 2019 is to define who is an 'e-consumer'. Certainly, without a concrete definition about an e-consumer one cannot even think about protecting e-consumers rights in the E-Commerce market. To enjoy the rights provided under the repealed Act as well as the recent CPA, 2019, it is necessary for an aggrieved person to fall within the definition of a consumer. This was

[7] Rediff.com India Ltd. v. Urmil Munjal, 2013 SCC OnLine NCDRC 348.
[8] Rajinder Chawla v. M/s Make My Trip India Pvt. Ltd., First Appeal No. 355/2013 (SCDRC Chandigarh, 22/08/2013).

certainly the biggest challenge which was posed before an aggrieved person prior to the new definition. The new definition of a consumer includes both online and offline purchases[9].

S. 2(7) of the CPA, 2019 defines a "consumer" as any person who—

(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment, when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or

(ii) hires or avails of any service for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such service other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person, but does not include a person who avails of such service for any commercial purpose.

The two category of consumers who are excluded from the purview of the Act are:

i. Any person who purchases any goods or avails any service for resale, or;
ii. For any commercial purpose.

The ambit of the term 'Commercial Purpose' has been slightly altered under the CPA, 2019 which excludes any goods bought and used exclusively for the purpose of earning one's livelihood by means of self-employment.[10] This certainly means that any person who buys goods or avails any services online for earning his livelihood will be governed by the provisions of the CPA, 2019.

[9] Supra 3, Explanation (b) of S. 2 (7).
[10] Supra 3, Explanation (a) of S. 2 (7).

(ii) Deficiency of Service: The E-Commerce entities prior to the enactment of CPA, 2019 could be held liable for deficiency of services only on limited grounds. However, the gap has been fixed under Section 2(11) of CPA, 2019, which in addition to any fault, imperfection or inadequacy in the quality, which is expected to be maintained and regulated in accordance with the law in force or in accordance with a contract/agreement undertaken by a person with respect to the products and goods, also includes any act of negligence or omission or commission and deliberate withholding of relevant information by such person due to which a consumer had to suffer loss or injury. The comprehensive definition will certainly protect the rights of the e-consumers too.

(iii) The Consumer Disputes Redressal Agencies: The Consumer Disputes Redressal Agencies were established under the CPA, 1986 to redress the grievances of the consumers, which at its inception was far beyond the foresight of the legislators about e-consumers. An aggrieved consumer can approach the consumer redressal agencies when there is a defect in goods or deficiency of services. The defaulted E-Commerce entities prior to the enactment of the CPA, 2019, were also brought under the unfair trade practices clause in the absence of a concrete legal provision. The CPA, 2019 has made a drastic change in the process of initiating a complaint, whereby any aggrieved consumer can register the complaint electronically.[11] In addition to e-filing of complaints the entire edifice of adjudication has been streamlined by authorizing District Forums and State Commissions to address, to review applications and also advice mediation wherever possible,[12] thus making the process time efficient which was the intention behind establishing consumer redressal agencies parallel to civil courts. The pecuniary jurisdiction of the three-tier redressal agencies has been enhanced one more time under the present CPA, 2019. The District Forum

[11] Ibid., S. 17.
[12] Ibid., S. 37.

is now entitled to hear disputes from claims of INR 1 crore or less; the State Commission can hear disputes from claims of INR 10 crores or less, and the National Forum to hear disputes above INR 10 crores. With the enhancement of the pecuniary jurisdiction of the District Forum to hear claims which do not exceed INR 1 crore rupees, it is evident that the number of complaints will also increase. To illustrate further, if 'A' is an e-consumer who has purchased a diamond set worth INR 75 lakh from 'Z' e-commerce website, 'A' needs to approach the District Forum first, and if not satisfied with the decision can then appeal to the State Commission and further to the National Commission. The entire process will consume more time of a consumer to get their rights redressed. Even under the CPA, 1986 the pendency of cases under the consumer disputes redressal agencies have drawn much attention. Additionally, the vacancies, infrastructural deficiencies added to the disadvantage. Efforts should be made to overcome the deficiencies which has been witnessed under the CPA, 1986. The CPA, 2019 certainly demands improved infrastructural requirements with internet connectivity to dispose of e-complaints. Even the members must undergo compulsory training to be familiar with the process of receiving e-complaints and disposing it off.

(iv) Online Consumer Mediation Centre: In order to redress the grievances of the e-consumers in India, the Online Consumer Mediation Centre was established at National Law School of India University, in 2016, under the aegis of the Ministry of Consumer Affairs, Government of India.[13] The objective of the Centre is to use mediation as a tool to resolve consumer disputes with e-commerce entities. The Centre is wholly dedicated to resolve e-commerce disputes through face-to-face mediation and online mediation. The medium of mediation to resolve consumer disputes has now been explicitly provided under the CPA, 2019. Resolving

[13] *The Consumer Grievance Redressal Mechanism of E–Commerce Sites*, National Law School of India University, available at https://clap.nls.ac.in/wp-content/uploads/ConsumerGuide/8E-COMMERCE.pdf, last seen 05/05/2021.

disputes amicably is better in many ways, it not only takes less time to arrive at an agreement, also saves money.

The CPA, 2019 has tried to fix the loopholes which existed under the CPA, 1986 with respect to the protection of consumer rights in e-commerce in India. The comprehensive rules which are required to be adhered to by an E-Commerce entity to carry on business in India is provided under the E-Commerce Rules. The next part of the paper critically analyzes the E-Commerce Rules which an E-Commerce entity, who is already carrying business in India or for any new e-commerce entity has to comply with while offering goods or services in India.

IV. THE CONSUMER PROTECTION (E-COMMERCE) RULES, 2020

1. To Whom are the E-Commerce Rules Applicable?

The governance of any e-commerce entity who directly or indirectly offers goods or services to consumers in India must necessarily abide by the E-Commerce Rules. The ambit of the E-Commerce Rules extends to all goods and services bought or sold over digital or electronic network including digital products; all models of e-commerce including marketplace e-commerce entities[14] and inventory e-commerce entities[15]; all e-commerce retail including multi-channel single brand retailers and single brand retailers in single and multiple formats; all forms of unfair trade practices[16] across all models of e-commerce.[17] According to sub clause (2) of Rule 2 of E-Commerce Rules, "*These rules shall apply to an e-commerce entity which is not established in India, but systematically offers goods or services to consumers in India.*" However, the word systematically is not defined and is open for interpretation. To cite an illustration, if a foreign website sells goods online and does not categorically offer its products only in India (which means

[14] Marketplace Entities are those entities which provide an information technology platform to facilitate transactions, while Inventory Entities own the inventory of goods/services and sell them directly to consumers. The E-Commerce Rules also apply to entities which are not established in India but systematically offer goods or services to consumers in India.
[15] Ibid.
[16] Supra 3, S. 2 (47).
[17] Rule 2 (1), The Consumer Protection (E-Commerce) Rules, 2020.

that it has a global outreach), it raises a moot point that whether these rules would be applicable on such websites. Certainly, these rules cannot be imposed on other nations without undergoing their process of ratification.

2. Consumer Complaints and Jurisdictional Aspect

The most pertinent issue concerning E-Commerce entities is the complex web or sequence of events, which extends to multiple countries and jurisdictions. For instance, it is possible to order a book online by a consumer present in India, while the seller, the server connection, and the headquarters of the Internet Service Provider are present in 3 different countries with different jurisdictions and all of these elements together make an online order possible. Therefore, dilemma arises as to where the consumer needs to seek redressal i.e., under which jurisdiction should a consumer take its grievance in case a dispute arises? The jurisprudence regarding jurisdictional issues where the defendant is not a habitual resident of the forum state, started developing in the United States ("**US**") and the European Union ("**EU**") in cases that are discussed below:

2.1 Jurisdictional aspects in the US

The doctrine of Minimum Contract, the primary rule regarding cross-border jurisdiction, was first established in the US through *International Show Co.* v. *Washington*[18]. It established a dual test in which the plaintiff, in order to show a sufficient 'minimum contracts' in the forum state, would have to establish that the defendant either purposefully directed, or purposefully availed itself of the privilege to conduct business in the forum state, or delivered one's product into the stream of commerce in the forum state. Moreover, the traditional notions of fair play and substantial justice must not be violated,[19] if the court assumes personal jurisdiction against the defendant. To show personal jurisdiction, sufficient ties or connections must be there between the forum state and defendant, and the minimum contracts doctrine is the litmus test to establish the same so that a

[18] International Show Co. v. Washington, 326 U.S. 310 (1945, Supreme Court of the United States).
[19] Ibid.

judgement can be passed *in personam*. Ultimately, the question is whether the defendant's 'minimum contracts' with the forum state can cause him to reasonably anticipate being sued in the forum state's Court. In *Burger King Corp* v. *Rudzewicz*,[20] it was held that the contracts referred to by plaintiff must not be random or fortuitous, but those contracts should result from *"actions by the defendant himself that created a substantial connection with the forum state."*

2.2 European Approach

The European approach is similar. Brussels I, an attempt to modernize the original Brussels Regulation, had a similar approach as discussed above.[21] Brussels I confirmed the conventional view that the consumer is the weaker party. According to Article 15(1)(c)[22] of the Regulation and also Article 6(1) of the Rome I Regulation[23], if the business targets its customers in a particular country, the business should be subject to the protective rules which either assign jurisdiction to that state or apply the national law of that state to govern the contract. Brussels I Regulation invokes the burden on the plaintiff to prove that the advertisement or online offer was specifically addressed towards the website user i.e., plaintiff. It suffices, for the purpose of the provision, that the online vendor directs its activities to the Member State, or any part of it where the consumer is domiciled. The above reasoning can be applied in case of India as well.

2.3 Indian Stance

The CPA, 1986 failed to resolve the cross-border e-commerce transactions as it did not contain any specific provisions to redress the same. Prior to

---

[20] King Corp v. Rudzewicz, 471 U.S. 462 (1985, Supreme Court of the United States).
[21] European Union, *Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*, O.J. L 12/1 (16/01/2001), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0044&from=EN, last seen on 05/04/2021.
[22] Ibid, Art. 15 (1) (c).
[23] Art. 6 (1*), European Union, Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)*, O.J. L 177/6 (04/07/2008), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0593&rid=2#d1e538-6-1, last seen on 05/04/2021.

the enactment of the CPA, 2019 the jurisdictional aspect was governed by the Information Technology Act, 2000. It was pertinent that the ambit of the CPA, 1986 be given a wider perspective to include within its clutches the e-commerce transactions which take place between a consumer in India and any other entity outside the territory of India. In India, Section 20 of the Civil Procedure Code, 1908 ("**CPC**") is the primary statutory provision responsible to govern jurisdictional questions related to civil matters. It states that a plaintiff could initiate an action either at the place where the defendant ordinarily resides or carries business or at the place where the cause of action arose.[24] The provisions of Section 20 of CPC are *para materia* to Section 34(2) (District Forum) and Section 47(4) (State Commission) of CPA, 2019. Thus, the rationale held in judgements suggestive of jurisdictional issues under Section 20 of CPC could be used as precedent in cases filed under consumer fora too as the consumer courts have now been granted jurisdiction to adjudicate over consumer complaints against e-commerce entities.

The applicability of Section 20 CPC was extensively used in *Banyan Tree Holding (P) Limited* v. *A. Murali Krishna Reddy*[25] ("***Banyan Tree***") which held that in absence of a "*long arm statute*", the plaintiff would have to show that the defendant "*purposefully availed*" itself of the jurisdiction of the forum court. A dual obligation is put forth on the plaintiff to prove the "*purposeful availment*", which encompasses that the defendant's use of the website was with an intention to commence a commercial transaction with the website user, and that such commercial transaction resulted in an injury or harm to the plaintiff, should occur within the forum court. The court in this case also held that:

> For the purposes of Section 20(c) CPC, in order to show that some part of the cause of action has arisen in the forum state by the use of the internet by the Defendant, the Plaintiff will have to show prima facie that the said website, whether euphemistically termed as "passive plus" or "interactive", was specifically targeted at viewers in the forum state for commercial transactions. The Plaintiff would have to plead this and produce material to prima

[24] S. 20, The Code of Civil Procedure, 1908.
[25] Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy, (2010) 42 PTC 361.

> facie show that some commercial transaction using the website was entered into by the Defendant with a user of its website within the forum state resulting in an injury or harm to the Plaintiff within the forum state.

Thus, a mere interactive website with no commercial activity whatsoever by the plaintiff in the forum state would not attract the jurisdiction of the forum state, as there has been no harm or injury *per se*. Moreover, it was held that the plaintiff had the burden to prove the intention of the defendant to conclude a commercial transaction with the website user.

A judgement which was indicative of the precedent of *Banyan Tree* and affirmed the decision held was that in *World Wrestling Entertainment Inc.* v. *M/s. Reshma Collection*[26]. *Inter alia*, the court observed that *"the availability of transactions through a website at a particular place is virtually the same thing as a seller having shops in that place in the physical world"* and thus held that it had the jurisdiction to entertain the suit. The same analogy can also be applied in case of jurisdictional disputes with respect to e-commerce transactions.

To ensure that the e-consumer rights are not affected due to the jurisdictional uncertainty, in addition to the insertion of specific provisions under the CPA, 2019, the E-Commerce Rules lays down a detailed provision to resolve such matter smoothly. The aspects relating to enforceability of the provisions of the E-Commerce Rules to the foreign business also remain to be clarified given that handling a dispute involving a foreign entity may have territorial and jurisdictional constraints. Through the E-Commerce Rules it would now be a mandatory provision for all the foreign entities who wish to carry on business in India to appoint a Nodal Officer who shall be the representative to redress the consumer grievances before bringing it before the Consumer Courts. This indeed would resolve the dispute with respect to jurisdiction.

3. Appointment of Nodal Officer

[26] World Wrestling Entertainment Inc. v. M/s. Reshma Collection, (2014) 58 PTC 52.

As pointed out in *Sri Kunal Bahl, Chief Executive Officer* v. *State of Karnataka,*[27] an intermediary as defined under Section 2(w) of the Information Technology Act or its directors/officers would not be liable for any action or inaction on part of a vendor/seller making use of the facilities provided by the intermediary in terms of a website or in a market place. Thus, directors/officers of marketplace E-Commerce entity cannot be held vicariously liable for the actions of third-party sellers if due-diligence[28] has been committed by the e-commerce entity to intimate seller of their rights and duties, as the E-Commerce entity cannot control and check all the goods which are being sold on the website.

As per CPA, 2019, to ensure compliance with the provisions of the Act or the E-Commerce Rules, an E-Commerce entity has an obligation to appoint a nodal officer of contact or an alternate senior designated functionary who is resident in India.[29] The E-Commerce Rules do not, however, set out any clarification if he will be vicariously liable, and the qualifications of such nodal officer are also not provided. This also will be an additional cost on the part of the E-Commerce entities who wish to offer goods or services to consumers in India. Whether the nodal person will be the point of contact for all the consumers from different parts of India who transact through e-commerce entity is something which is not clearly provided in the E-Commerce Rules. It would certainly be important for the nodal officers to be well versed with varied languages as the consumers would generally be comfortable in conversing in their native language. The nodal officers will be under an obligation to resolve the disputes within a period of one month after acknowledging the complaint within 48 hours[30] which is a welcome provision to restrict the number of cases to go before the redressal agencies.

4. Consent of the Consumers

[27] Sri Kunal Bahl v. State of Karnataka, Crl.P. No. 4676 & 4712 of 2020 (Karnataka High Court).
[28] Rule 3, Information Technology (Intermediary Guidelines) Rules, 2011.
[29] Supra 16, S. 4 (1) (a).
[30] Ibid, S. 4 (5).

Before the enactment of the E-Commerce Rules, the e-consumer had to mandatorily accept the terms and conditions of the E-Commerce entity, if he chooses to purchase a good or avail any services. The consent of the E-Consumers was not taken into consideration. Under the CPA, 1986, consumers did not have a choice but to consent to the checkboxes provided. Rule 4(9) is a welcome provision where it makes it mandatory on every E-Commerce entity to only record the consent of a consumer for the purchase of any good or service offered on its platform where such consent is expressed through an explicit and affirmative action thus doing away with the practice of recording the consent automatically in the form of pre-ticked checkboxes.

For the consumers to make an informed choice at the pre-purchase stage from market E-Commerce entities, Rule 5(d) of the E-Commerce Rules has made it an obligation to highlight the 'country of origin' of the goods. However, the challenge will be when a single product has multiple 'country of origin'. Also, the E-Commerce Rules are not applicable to inventory e-commerce entities.[31]

5. Cancellation Charges

Rule 4(8) intends to provide equal liability on both the consumers and the entity in terms of imposing cancellation charges. Unless the E-Commerce entity is ready to bear similar expenses when they cancel any order unilaterally for any reason, they are prohibited to impose any cancellation charges on the consumers as well. However, the imposition of cancellation charge should be something which needs to be decided on case-to-case basis depending upon the genuineness of the reasons cited.

6. Grievance Redressal Mechanism of Service provider

The first step that an aggrieved consumer should think of is approaching the competent Grievance Redressal Mechanism or regulatory bodies

[31] PTI, *Delhi HC asks govt to verify if e-commerce sites display country of origin on products*, The Print, available at http://theprint.in/judiciary/delhi-hc-asks-govt-to-verify-if-e-commerce-sites-display-country-of-origin-on-products/563720/, last seen at 24/12/2020.

maintained by the service providers only. For instance, many companies and organizations have their internal grievance redressal mechanism and before resorting to legal means against the service provider, an aggrieved consumer can approach this mechanism, which has a dual advantage of being cost and time effective. In order to circumvent the judicial process of consumer complaint, the aggrieved consumer could also send a legal notice to the service provider encompassing all the essential details such as particulars of complaints, relief sought, and any other detail necessary to be brought before the service provider. However, as this action is not essential, the consumer could directly approach the consumer court too. The advantage of sending a legal notice prior is the chance of effective settlement in timely manner of both the consumer and service provider, as the complaint might get resolved prior to availing statutory remedies which is a very lengthy process. However, if the service provider disregards the notice, the complainant has the right to file a legal compliant.

IV. CONCLUSION

The CPA, 2019 is a welcome legislation to deal with the complexities arising out of transactions in the digital market which the CPA, 1986 failed to deal with. The benevolent and beneficial legislation intends to protect the rights of the consumers not only from defect in the goods or deficiency in services, but also from misleading facts, advertisements and from unfair trade practices. The expansion of the ambit of this legislation to both national and foreign e-commerce entities has made its applicability extra-territorial in nature by making it an obligation for any e-commerce entity who wishes to offer goods and services to the consumers in India to comply with the provisions of the CPA, 2019 and the E-Commerce Rules framed in that regard. The mandatory requirement on the part of an E-Commerce entity to appoint a Nodal officer to deal with the consumer complaints, can help reduce the burden on the Consumer Disputes Redressal Agencies as most of the complaints can be now resolved in the bud by the Nodal officers. However, it does not prohibit any consumer from approaching the Courts without approaching the Nodal officer. Since

the Nodal officer will act as a mediator between the consumer and the e-commerce entity, it is pertinent that the position shall be occupied by a person who possesses the requisite skills and qualifications to resolve disputes. However, the E-Commerce Rules have failed to provide the qualifications which a Nodal officer has to possess. Also, in case if an E-Commerce entity fails to comply with any of the Rules, can the Nodal officer be held vicariously liable? The E-Commerce Rules are silent with respect to such a situation. Thus, the liability of the Nodal officer needs to be clearly stated. Additionally, the dispute with respect to jurisdiction in cross-border e-trade certainly poses as an impediment in providing speedy justice to the consumers. The awareness amongst the consumers about the provisions of the Act as well as the Rules will help in proper implementation of the Act. Since the E-Commerce Rules are novel to both the consumers as well the E-Commerce entities, we need to wait and watch whether the e-commerce entities have made the necessary changes to carry on their business in India in a consumer-friendly manner. The e-commerce entities also need to comply with the requirements under certain other legislations as mentioned. It can be concluded that the E-Commerce entities will be booked for violation of the provisions under the CPA, 2019 and for failing to comply with the E-Commerce Rules framed by the Central Government. However, the success of the Act will depend upon overcoming the hurdles faced during the enforceability of the Rules, also the awareness and vigilance amongst the consumers about their rights and due procedures established to protect them in the digital market in India.

ARTICLE SUBMISSION AND REVIEW POLICY

- **Exclusive Submission Policy**

A submission sent in for our review must not be submitted elsewhere. Once published or accepted for publication in our review, a submission becomes the copyright of the RGNUL Student Research Review and the author in a manner that is prejudicial to our copyright must not deal it with. All authors must conform to the exclusive submission policy and all submissions made to the review must be on the understanding that the authors have agreed to the stipulation.

- **Indemnity for Liability**

The author also undertakes to indemnify the Review from any action or suit arising out of the publication of a submission proffered by the author in favor of the review. While the Review does a comprehensive study of all submissions placed before it and published by it, the final liability shall always rest with the author.

PUBLISHED BY:
The Registrar
Rajiv Gandhi National University of Law, Punjab
Sidhuwal-Bhadson Road, Patiala
Email: rslr@rgnul.ac.in
Web URL: www.rsrr.in