

INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

Volume 3 | Issue 3

2025

Website: www.ijlae.com

Email: editor@ijlae.com

LEGAL SAFEGUARDS FOR CONSUMERS IN E-COMMERCE: A COMPARATIVE PERSPECTIVE FROM INDIA AND THE UNITED STATES

Debdipa Bera

***Research Scholar, Department of Legal Studies, Banasthali Vidyapith,
Rajasthan***

&

Dr. Preeti Sanger

***Assistant Professor, Department of Legal Studies, Banasthali Vidyapith,
Rajasthan***

ABSTRACT

We are living in an era where Consumer protection, especially for consumers dealing in E-commerce transactions, has become an emerging issue. The consumers, unless well-protected by law, will be exploited in the Online Marketplace. In both traditional and online buying and sale contracts, consumer protection should be the primary focus of business entities. Though there are several laws regulating consumer protection, up to now there are still rampant violations of consumer rights, particularly in e-commerce transactions. In such a situation the consumer laws of a nation must be stringent enough to make sure that the consumers are safeguarded and aren't vulnerable to deceptive and misleading marketing practices.

The authors of this paper will try to compare the Consumer Protection Laws of India and the United States and analyse the differences between the two in terms of the protection of consumers in E-commerce sector. In addition, this research gives suggestions on how legal certainty for consumer protection in e-commerce transactions in India ought to be when considered from the comparison of consumer protection laws in e-commerce transactions in the United States. The analysis further extracts some recommendations to make the consumer laws stricter in India in an attempt to decrease unfair trade practices further.

Keywords: *Consumer laws, E-commerce, India, United States, Consumer protection, Comparison.*

INTRODUCTION

In India, the Consumer Protection Act of 2019 and the Consumer Protection (E-commerce) Rules created in 2020 provide a vital set of guidelines to protect the rights of online consumers. These rules are intended to promote greater transparency and accountability in e-commerce transactions to make sure that consumers are adequately informed about their purchases. The act focuses on essential consumer rights, including the right to be informed, the right to seek redressal against grievances, and the right to be heard. The legislative structure seeks to empower consumers through enabling them to be equipped with necessary tools against unfair trade practices and frauds.

Conversely, the United States utilizes a patchwork of state and federal statutes to oversee consumer business in the e-commerce arena. Among these, the Federal Trade Commission (FTC) Act is preeminent, banning unfair and deceptive business acts in online commerce.¹ The regulations of the FTC are supplemented by numerous state laws that also focus on consumer protection, each having its own individual set of requirements and enforcement methods. Together, these laws strive to create a safe and fair online marketplace for consumers, mandating that businesses uphold ethical standards and maintain clarity in their advertising and service delivery.

REGULATORY ENVIRONMENT IN INDIA

The Consumer Protection Act 2019:

The Consumer Protection Act 2019 is a holistic piece of legislation that aims to protect the rights and interests of Indian consumers. It not only puts focus on consumer protection but also sets up dedicated bodies that are in charge of the timely and effective redressal of consumer grievances. It sets up mechanisms for redressal, whereby grievances are quickly and effectively redressed, hence creating a level playing field in the marketplace. In addition to this, such

¹ Maggs GE, "Regulating Electronic Commerce" (2002) 50 The American Journal of Comparative Law 665 <<https://doi.org/10.1093/ajcl/50.suppl1.665>>

legislation also imposes certain rights upon consumers, i.e., their right to wholesome and healthy conditions of life, their right to information, as well as the right to file claims for injuries suffered. Such an initiative benefits consumer by allowing them to act with confidence over the products they buy.

The Consumer Protection Act of 2019 is responsible for the law on consumer protection in India. It is specifically governed for e-commerce transaction under E-Commerce Rules 2020.² The term e-commerce is defined under Section 2 of the Consumer Protection Act 2019 as selling or purchasing of goods or services including digital products on digital or electronic network. Marketplaces and online auction sites are also covered under the regulation under the Consumer Protection Act 2019, which too mandates the consumer protection law. One of the most significant differences between Indian and Indonesian consumer protection laws is in terms of consumer protection institutions. India does acknowledge the presence of the Central Consumer Protection Authority ("CCPA"), as it is governed in Sections 10 to 27 of the Consumer Protection Act.³ The CCPA is an organisation appointed by the Central Government of India to handle cases that are pivotal to the welfare of consumers, including unfair trade practices and misleading advertisements. Furthermore, the CCPA also works to safeguard and protect consumer rights. The CCPA consists of the Chief Commissioner, other commissioners appointed by the Central Government and investigation agencies. The organization of CCPA investigative body includes a director general who oversees search and seizure. The Consumer Protection Act also has provisions for the protection of consumer data privacy. Section 2 provides what would be an unfair business practice with the disclosure of consumer personal information by a business, seller or service provider without the consent of the consumer.⁴ As per these provisions, the Consumer Protection Act 2019.

Consumer Protection (E-commerce) Rules, 2020:

These rules have been brought forth with the primary motive of specifically regulating online purchasing transactions, clarifying key consumer rights and e-commerce platform duties. The norms have emphasized bolstering transparency, establishing consumer safety measures, and allocating liabilities on misrepresentative fronts.

² Advocate AJAJ, *The Consumer Protection Act, 2019 Alongwith (The Consumer Protection Rules & Regulations 2020)* (Abhishek Publications 2020)

³ India, Consumer Protection Act of 2019, ss 10-27

⁴ India, Consumer Protection Act of 2019, s 2

Provisional Guidelines

1. **Accountability and Transparency:** E-commerce sites are required to provide detailed and accurate information on the products presented, the entities selling these products, and returns and exchange policies. This consists of in-depth descriptions of the features of a product, cost structures, as well as the conditions associated with purchases.⁵
2. **Grievance Redressal Mechanism:** In order to enhance consumer trust, the e-commerce entities shall have sound systems in place for the prompt resolution of consumers' grievances.⁶ This includes channelized mechanisms of complaints, timeframe for resolution and transparency in follow-up procedures while keeping the consumers updated during the process.
3. **Refrain from Unfair Trade Practices:** The Act clearly prohibits unfair trade practices through misleading advertisements or false information.⁷ It also targets unfair pricing through hidden charges and overcharging of prices.
4. **Product Authenticity Guarantee:** It is the duty of e-commerce platforms to ensure the authenticity of the products being sold on their websites.⁸ This involves intensive screening of sellers and products, giving assurance that the consumers obtain true representations in product description and that the advertised product is actually available.
5. **Protection of Data and Privacy:** With the increasing concern for security of personal information, these laws emphasize the importance of ensuring the safety of consumer data. E-commerce players must adopt robust data protection practices for ensuring customer data confidentiality and security and protecting it from unauthorized access and data leakage. In general, the regulations are meant to develop a more secure and credible e-commerce environment, empowering consumers with the rights and protections they need.

Requirements for Displaying Information by Sellers:

Sellers must give clear and detailed information to consumers about their products and services. This entails:

- **Total Price:** The total amount of the product or service must be clearly stated, so consumers know the overall figure they will pay.⁹

⁵ India, E-Commerce Rules of 2020, Rule 5

⁶ India, E-Commerce Rules of 2020, Rule 5

⁷ India, E-Commerce Rules of 2020, Rule 6

⁸ India, E-Commerce Rules of 2020, Rule 7

⁹ India, E-Commerce Rules of 2020, Rule 6(5)(b)

- Breakdown of Charges: All charges that may be applicable, such as taxes, shipping costs, and service fees, must be given in an itemized form to increase transparency.¹⁰
- Mandatory Notices: Legally mandated notices or disclaimers must be included to provide consumers with information about their rights and responsibilities.¹¹
- Expiry Dates: Where relevant, sellers are required to include the dates of expiration for perishables or products with low shelf life so that consumers can make informed purchasing decisions.¹²
- Details About the Goods: Detailed descriptions of the product such as specifications, materials, and use instructions must be conveyed in a clear manner.¹³
- Country of Origin: Details of where the product was made or sourced are critical, letting consumers know the origin of the product.¹⁴
- Contact Information for the Grievance Officer: Sellers should give contact details of a grievance officer or customer service person to deal with complaints or queries from consumers.¹⁵
- Terms for Returns and Refunds: Transparent policies on returns and refunds need to be given, detailing the process and conditions of eligibility.¹⁶
- Delivery and Shipment Information: Customers should be provided with details regarding shipping options, charges, delivery time estimates, and tracking possibilities.¹⁷

Other Applicable Laws:

Information Technology Act, 2000 (IT Act):

The IT Act was the first piece of legislation in India to target cybercrimes and online commerce. Sections 43A¹⁸ and 72A¹⁹ address data protection specifically, requiring organizations to ensure

¹⁰ India, E-Commerce Rules of 2020, Rule 6(5)(b)

¹¹ India, E-Commerce Rules of 2020, Rule 6(5)(c)

¹² India, E-Commerce Rules of 2020, Rule 6(5)(c)

¹³ India, E-Commerce Rules of 2020, Rule 6(5)(d)

¹⁴ India, E-Commerce Rules of 2020, Rule 6(5)(d)

¹⁵ India, E-Commerce Rules of 2020, Rule 6(5)(e)

¹⁶ India, E-Commerce Rules of 2020, Rule 6(5)(g)

¹⁷ India, E-Commerce Rules of 2020, Rule 6(5)(h)

¹⁸ India, Information Technology Act, 2000, s43A

¹⁹ India, Information Technology Act, 2000, s72A

reasonable security practices to protect consumer data. Section 66E further prescribes penalties for privacy violations.

Established by the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, also known as the CERT Rules, the Computer Emergency Response Team (CERT-In) is set up to collect, correlate, and disseminate information regarding cyber incidents, among other things, and take appropriate emergency measures to prevent these.

The Digital Personal Data Protection (DPDP) Act of 2023:

The Digital Personal Data Protection Act, 2023 is an Act of India enacted for the processing of digital personal data in such a way that it acknowledges both the right of individuals to guard their personal data and the requirement to process such personal data for legal purposes and for matters incidental thereto or connected therewith.

REGULATORY ENVIRONMENT IN THE USA

Federal Trade Commission (FTC) Act:

This landmark legislation is the cornerstone of consumer protection in the United States, particularly in the context of e-commerce. It requires fair business practices, advertising truthfulness, and protection from deceptive acts.²⁰

Major Provisions:

- **Accuracy of Product Descriptions:** Sellers are required to ensure that all product descriptions are not only accurate but also truthful in order to avoid misleading consumers.
- **Disclosure of Terms and Conditions:** Sellers are required to clearly disclose terms and conditions applicable to purchases, such as warranty information and return procedures.
- **Respecting Warranties and Return Policies:** It is a requirement for vendors to honor their expressed warranties and return policies in order to ensure consumer rights.

State-Level Legislation:

²⁰ The United States of America, Federal Trade Commission Act, Section 5, (15 U.S.C. § 45)

Besides federal legislation, various states have adopted their own consumer protection laws that might address specific products or problems not covered by federal legislation, further enhancing consumer rights and safeguards.

Other Applicable Laws Are:

- Federal Food, Drug, and Cosmetic Act: This act guarantees the safety and proper labeling of food, drugs, and cosmetics, ensuring consumer health and safety.
- Fair Debt Collection Practices Act: This act helps protect consumers from abusive and oppressive practices in debt collection, providing concrete guidelines for debt collectors.
- Fair Credit Reporting Act: It oversees the collection, use, and disclosure of consumer credit information, providing consumers with rights to their credit information.
- Truth in Lending Act: This act requires lenders to clearly state the terms, interest rates, and charges of loans so consumers can make enlightened financial choices.
- Fair Credit Billing Act: Grants consumers protection from unjust billing practices on credit accounts, ensuring a fair credit system.
- Gramm–Leach–Bliley Act: The act protects consumer financial data, setting standards for privacy and use of data by financial institutions.

Federal Laws Regulating Unsolicited Emails, SPAM, and Spyware:

As email became more and more popular after the turn of the millennium, lawmakers became concerned about the potential for consumer abuse in the form of unsolicited or fraudulent emails.

In 2003, Congress enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, more commonly referred to as the CAN-SPAM Act. This legislation is an evolution of federal e-commerce consumer protection legislation, which had been targeted up until that point to telephone solicitations and the almost antique fax machine. The CAN-

SPAM Act only applies to e-mails that are sent as a commercial advertisement or a promotion of commercial products or services.²¹

All companies that send commercial or unsolicited emails should be familiar with the provisions of the law. In the first place, CAN-SPAM prohibits placing false or misleading subject lines in emails. The law also mandates that the subject line be truthful and the message be identifiable. CAN-SPAM also mandates that the sender place its postal address in the subject matter and inform recipients of their right to opt out of future mailings. The law mandates that the sender respect those opt-out requests within ten days of receipt and it has an anti-charging provision for the service.²² CAN-SPAM also bars the sale or transfer of an email address belonging to a recipient, with limited exceptions. Lastly, the law bars organizations from circumventing the law.

An illustration could be, that if a business advertises a product through email, but relies on a third party to do so, in this third party the business retains legal responsibility for the third party's actions. CAN-SPAN is purposefully an amazingly comprehensive set of anti fraud provisions to penalize and deter abuse of the email medium. Statutory offenses under the statute are penalized in severe, with fines exceeding \$40,000 per offense. CAN-SPAM also makes a distinction between commercial messages and transactional messages. When deciding whether an email has a primary business purpose for the statute, regulators take hold of the view of a regular consumer perusing the subject line of an unjustified message.

An email is in the scope of commercial email if the recipient would probably read the subject line as being for a commercial promotion / ad of any kind. An email that is related to any transaction with an organisation is refer to as transactional character, however the message content of such an email should be connected to some transaction a customer has made with any association, for example, product guarantee, recall or some other context which requires notice (e.g. notice on changes of the terms in an arrangement, provide account balance details or provide any good or administrations which the purchaser has allowed himself to receipt of). CAN-SPAM excludes the bulk of the primary CAN-SPAM restrictions on transactional emails. The Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act (sometimes referred to just as the SAFE WEB Act of 2006) is another major law

²¹ Mathis M, "Can You Get in Trouble for Sending Unsolicited Emails?"

<<https://guardiandigital.com/resources/faq/can-you-get-in-trouble-for-sending-unsolicited-emails>>

²² Serna FJA, "The Legal Regulation of Spam: An International Comparative Study" (2022) 3 Journal of Innovations in Digital Marketing 1 <<https://luminousinsights.net/articles/jidm-2022-44>>

that protects consumers online. Among other things, SAFE WEB aims at "combatting spam, spyware and Internet fraud and deception". This legislation is merely extending existing computer fraud and abuse act policy along with policy contained in the CAN-SPAM Act.

Unlike other acts that had only targeted consumer fraud at a national scale, the SAFE WEB Act was designed to address foreign fraud concerns in an attempt to protect US consumers.

SAFE WEB provides valuable consumer protection concerning spyware, spam, and other forms of internet assaults, which is an expanding concern around the globe.²³ Regulators in 2004 processed in excess of 860,000 complaints concerning spam, spyware, and online fraud. This number grew by 2014 to three times as much in excess of 2.5 million complaints.

These statistics stand as powerful rationale for further legislation and regulation battling internet fraud. To assist in alleviating the problem, the SAFE WEB Act broadens the FTC's authority to counter international computer fraud against United States residents. For instance, the SAFE WEB Act allows the Federal Trade Commission to pass on its confidential information to overseas law enforcement agencies. This enables the agencies to collaborate with overseas law enforcement officials to assist in stemming internet activity facilitating international fraud. This collaboration makes possible more thorough policing of international illegal activity and encourages other nations into sharing reciprocal information.

Online Retail Consumer Protections:

All of these laws all shield some facet of online consumer behaviour. Legislation has been enacted on the books dealing with AI-restricted access to consumer financial data, hacking and computer fraud and commercial solicitation for purposes of advertising made over email. The laws and regulations that deal with online retail consumers are another significant sector.

Congress followed with the Restore Online Shoppers' Confidence Act, or ROSCA, in 2010 to further develop safeguards for consumers who shop for products online.²⁴ ROSCA complements gaps in the expanding arena of online consumer protection. One of the laws that enforce a process like data pass is an example, which is where an internet consumer buys from a first merchant but that merchant passes along a third party to handle the transaction. This is

²³ Zhu S, "Does the U.S. SAFE WEB Act Strike the Proper Balance between Law Enforcement Interests and Privacy Interests?" (*UW Law Digital Commons*) <<https://digitalcommons.law.uw.edu/wjlta/vol5/iss1/5/>>

²⁴ Bertoni D, "ROSCA: The Restore Online Shoppers' Confidence Act -" (*Brann & Isaacson*, January 26, 2021) <<https://www.brannlaw.com/eyes-on-ecom-law/rosca-restore-online-shoppers-confidence-act-2010/>>

left uncontrolled, thus allowing the third party an opportunity to sell the consumers' information and make money off the unknowing customer's information. To prevent the sale of individual retail consumer information the law prohibits the data passing that would otherwise permit ROSCA.

ROSCA also places requirements on negative option features. A negative option feature is how the Federal Trade Commission defines an offer to sell goods or services that includes a term stating that the customer's silence or not refusing the goods or services indicates treatment as an acceptance of the offer. Those firms which offer negative option and are dependent on customers forgetting or not noticing that they are being charged continuously for them. Negative option features are usually used when a firm offers a customer a free service or product in exchange for such a person's credit or debit card details during the time of registration. After this, the consumer is now enrolled in a subscription plan or membership.

The negative option feature with ROSCA does not have any restrictions or criminality. Instead, the act ensures that sellers operating online guarantee that the customers signing up for the plans purpose to do so. Therefore, ROSCA forbids a company to hit upon a negative option campaign nor start it without the clearly and conspicuously set out all the material terms of the transaction prior to the customer providing the billing information.²⁵

The business also needs to obtain, before charging some one's account, an informed consent of the consumer and should have simple means for consumers to prevent unwanted recurring charges. Like a suite of other federally outsourced consumer defense legislation, ROSA gives 1000000000.00 dollars for anybody who does not follow the law. This penalty may be up to \$16,000 per offense and restitution payments and any equitable relief necessary to place the victimized consumers in the position in which they were prior to such activities.

Administrative Regulations to Protect Online Consumers:

Two of the most important executive agencies that take care of online consumers, the Federal Trade Commission or the "FTC" and the Federal Communications Commission or "FCC," are in action.²⁶ Initially, those two agencies worked independently but in time it became necessary

²⁵ Chargebacks, "What Is the Restore Online Shoppers' Confidence Act?" (*Chargebacks911*, January 30, 2025) <<https://chargebacks911.com/restore-online-shoppers-confidence-act/>>

²⁶ "FTC and FCC Sign Memorandum of Understanding on Continued Cooperation on Consumer Protection Issues" (*Federal Trade Commission*, August 20, 2024) <<https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-fcc-sign-memorandum-understanding-continued-cooperation-consumer-protection-issues>>

for the jurisdictional agreement as to each agency's roles and responsibilities with respect to consumer complaints against the internet service providers. Consequently, in December 2017 the agencies put in place a formal agreement to coordinate their efforts to better defend online consumers. The agreement shows new policy initiatives which have been enacted under the Trump administration, specifically about the shifts in online consumer protection that have come as a result of the new leadership's policy shift. Most significantly, this involves the "Restoring Internet Freedom" Order that de facto overturned the Obama administration's sweeping net neutrality policy. Overall, the Federal Communications Commission during the Trump administration has applied a "light touch" to regulating internet business, opting instead to foster creativity and innovation by loosening the previously expansive standards concerning internet consumer access.

As it regards areas of responsibility on-line, the FCC and FTC have a shared licensing authority for the area of consumer protection, while the memorandum of understanding between the agencies redistributes functions and responsibilities based on the mandates of the agencies. For instance, under the mandate's requirements, the FCC is obliged to make the communications on-line open. The agency will police on-line markets to meet this obligation and will be policing what might be restrictive business practice. It includes looking into informal complaints by consumers, if needed and investigating the same.²⁷ But, online commerce unfair and deceptive business practices are handled by the FTC. Thus, while the FCC was required to examine the consumer complaints, the FTC investigated and punished those it confirmed had violated applicable laws.

Focusing on consumer protection in online advertising, the FTC also imposes a set of rules, and in addition to cooperative enforcement of the online consumer protection laws, created under the agreement between the FCC and FTC — there is agreement to cooperate in that regard — and those set of laws, it also has its own set of rules. Finally, the FTC released its Dot Com Disclosures guidance in 2000 after public commenting and notice. Even though the details of the FTC's Dot Com policies described in Module 1 are explored in more detail, I must mention that the agency is very strict regarding the form and the content of material distributed through e-commerce in order to prevent the acts or the concealment of information from being unfair or misleading. The FTC requires all online advertisements and other

²⁷ Raul AC and Mohan VK, "FTC & FCC Memorandum of Understanding on Consumer Protection" (*Lexology*, December 14, 2015) <<https://www.lexology.com/library/detail.aspx?g=3ebef941-3837-4dd3-8861-ac67f386a166>>

commercial messages to be clear and conspicuous so that consumers will not be deceived or misled by the advertisements.²⁸ This is a subjective standard, which means that the issue of whether a specific piece of information presented in e-commerce is deceptive or unfair depends on the customer's point of view. Representations of commercial goods or services presented on the Internet should be readily seen and comprehended by the common consumer, and the agency would put the obligation on the proprietor of the site to guarantee fair and precise data for consumers. These efforts can give added strength to the legal landscape that protects Indian consumers in the ever-changing context of Indian e-commerce, with India drawing an inspiration from America by formulating thorough and purposeful regulations.

COMPARISON AND SUGGESTIONS TO INCORPORATE US LEARNINGS IN INDIAN PERSPECTIVE

Those rules mentioned above would address key concerns like data privacy, making sure that personal data is carefully safeguarded, deceptive advertising that can mislead consumers, and efficient mechanisms for resolving disputes that enable conflicts to be resolved promptly and justly. In addition, it is important to establish clear jurisdictional lines and enforceable mechanisms to instil confidence among consumers and businesses alike, providing a safe and reliable online marketplace.

Here's a more detailed breakdown:

1. Addressing Key Challenges:

False Advertisements and Misleading Claims:

Indian laws regarding e-commerce need to be fortified with strict provisions aimed at fighting and punishing false claims as well as deceptive advertising practices against products or services. Similar to the US, these steps will help empower the consumers and inculcate faith in the marketplace.

Data Protection and Security

²⁸ Hayes A, "Federal Trade Commission (FTC): What It Is and What It Does" (*Investopedia*, April 21, 2022) <<https://www.investopedia.com/terms/f/ftc.asp>>

Along with international standards, India must adopt robust data protection legislation and enforceable mechanisms that ensure the privacy and security of consumer information collected during e-commerce transactions. This will not only safeguard people but also instill confidence in online shopping.

Product Quality and Safety:

Regulatory frameworks should be established to hold e-commerce platforms accountable for the quality and safety of the products they offer, reflecting the high standards found in the US. Ensuring that consumers receive safe and reliable products should be a top priority for any online marketplace.

Return and Exchange Policies:

It is necessary to have clear and enforceable policies on return and exchange. The policies should be framed to ensure that consumers are provided with a reasonable and uncomplicated procedure to address their discontent, providing peace of mind for each purchase.

Dispute Resolution:

The establishment of effective and accessible dispute resolution mechanisms is crucial, such as the use of online platforms for the resolution of consumer complaints. These mechanisms will enable consumers to be heard and their concerns resolved quickly.

Jurisdiction and Enforcement:

Having well-defined criteria for resolving e-commerce disputes, especially those dealing with cross-border transactions, is important. Also, facilitating effective enforcement of consumer protection law will enhance the integrity of the entire e-commerce market.

Learning from US Practices:

FTC Model: Learning from a Strong Framework

India can benefit immensely by following the Federal Trade Commission's (FTC) critical function in enforcing consumer protection legislation in the United States. The FTC has the remarkable power to investigate and prosecute fraudulent acts, serving as a protector of consumers in the marketplace.

Regulations Customized for E-commerce

The U.S. has developed niche laws directly addressing the fast-paced era of e-commerce, including the Children's Online Privacy Protection Act (COPPA) and the Do Not Track features. These clearly defined laws protect the most susceptible consumers online and could be pragmatically customized to India's distinct online ecosystem.

Highlighting Transparency and Disclosure:

American laws put the spotlight on transparency and openness. Online businesses are required to provide detailed and clear information about their products, services, and terms of sale, instilling confidence and trust in consumers.

Data Privacy and Security: Protection of Personal Information

During an era in which data breaches are startlingly prevalent, the U.S. has put forth strong data privacy legislation, like the California Consumer Privacy Act (CCPA). India could also do well to look at equally strong frameworks while it develops its own data protection policies to safeguard citizens' private data.

Product Liability: Keeping Companies Accountable

In the United States, robust product liability rules make companies accountable for defective products, making consumer safety paramount. This can become a foundation for India's regulations on e-commerce, increasing accountability and responsibility in the market.

Improving Legal Certainty: A Way to Clarity

- **Unambiguous and Uncomplicated Laws:** It is necessary that regulations related to e-commerce are put into words clearly and simply so as to minimize vagueness among businesses as well as customers. This provides an avenue towards easy comprehension of responsibilities and rights.
- **Standardized Enforcement Mechanisms:** Having uniform enforcement mechanisms in place will guarantee that consumer protection legislation is enforced uniformly across different e-commerce sites and geographical locations, providing a level playing field for everyone.
- **Public Awareness Campaigns:** Initiating mass public awareness campaigns will empower consumers, making them aware of their rights and obligations in the context of e-commerce transactions. Knowledge is the key to successful participation.

- **Industry Collaboration:** Through engagement with e-commerce companies, a compliance culture and self-regulatory environment can prevail, producing a collaborative climate in which industry participants assume an active role in enforcing consumer protection standards.
- **Regular Review and Updates:** To remain in sync with the constantly changing digital world, it is essential to regularly review and update e-commerce laws. This continuous process will ensure that such laws respond to emerging issues and continue to be applicable in a dynamic world.

CONCLUSION

Over the past three decades, federal legislation has forged a formidable framework of online consumer protections, meticulously designed to govern the myriad activities that consumers engage in within the digital realm. Yet, as technology continues its relentless march forward, these laws must be regularly evaluated and adapted to meet the evolving needs of online consumers. The future viability of our present enforcement tools for protecting consumers on the Internet is uncertain, and this forces Congress to consider whether to enact new legislation to address pressing concerns like consumer privacy and the constant potential for fraud.

When it comes to online buying, consumer satisfaction and confidence are overriding concerns. Strong legislation that inflicts severe punishment on offenders, as well as streamlined procedures for resolving complaints, can make consumers confident enough to adopt online shopping. Over and above the attractive deals and discounts offered by e-commerce sites, it is the strength of legislation that will drive the expansion of the e-commerce industry. The governments need to focus on legislating robust laws to strengthen the pillars of this emerging industry.

When drawing comparisons with the United States, it becomes evident that India lags behind in addressing consumer protection and e-commerce dynamics. For example, although the principle of product liability was introduced in the U.S. for the first time in 1972, India incorporated similar provisions only in 2020. The United States has strict consumer rights protection, including a wide range of laws like the Consumer Credit Protection Act, the Consumer Product Safety Act, and the Children's Online Privacy Protection Act, among others.

These laws manifest a strong commitment to protecting consumer interests and the assurance of accountability.

In this era of accelerated digitalization, the need for India to create and implement stronger laws against online fraud has never been more urgent. This dedication to strong consumer protection not only protects the rights of people but also acts as a spur to the growth of e-commerce, creating a climate where security and trust lead to innovation and development.