MAPPING THE LEGAL AND REGULATORY FRAMEWORKS OF THE AD-TECH ECOSYSTEM IN INDIA

April 24, 2025

By VIPUL KHARBANDA

Reviewed by- PALLAVI BEDI

TABLE OF CONTENTS

INTRODUCTION AND SCOPE

The main purpose of regulations in any sector is essentially twofold, one is to ensure that the interests of the general public or consumers are protected, and the other is to ensure that the sector itself flourishes and grows. Too much regulation may possibly stifle the commercial potential of any sector, whereas too little regulation runs the risk of leaving consumers vulnerable to harmful practices.

In this paper, we try to map the legal and regulatory framework dealing with Advertising Technology (Adtech) in India as well as a few other leading jurisdictions. Our analysis is divided into three main parts, the first being general consumer regulations, which apply to all advertising irrespective of the media – to ensure that advertisements are not false or misleading and do not violate any laws of the country. This part also covers the consumer laws which are specific to malpractices in the technology sector such as Dark Patterns, Influencer based advertising, etc.

The second part of the paper covers data protection laws in India and how they are relevant for the Adtech industry. The Adtech industry requires and is based on the collection and processing of large amounts of data from the users. It is therefore important to discuss the data protection and consent requirements that have been laid out in the spate of recent data protection regulations, which have the potential to severely impact the Adtech industry.

The last part of the paper covers the competition angle of the Adtech industry. Like with social media intermediaries, the Adtech industry in the world is also dominated by two or three players and such a scenario always lends itself easily to anti-competitive practices. It is therefore imperative to examine the competition law framework to see whether the laws as they exist are robust enough to deal with any possible anti competitive practices that may be prevalent in the Adtech sector.

CONSUMER ADVERTISING

The purpose of advertising is to inform the consumers about the advantages of goods and services being sold and thereby increasing sales. It is therefore obvious that if left unchecked, advertising claims may become devoid of reality in order to inflate and magnify the qualities of the products being sold so as to increase sales. Traditional advertising regulations were put in place to check such malpractices and ensure that advertising content itself was not harmful to the public and did not violate the morals of the society. These regulations traditionally provided that advertising should be truthful and comply with the accepted standards of public decency. These provisions however have had to be supplemented with provisions catered specifically to prevent misleading practices in the digital advertising sector, as will be discussed below.

Indian Regulations

Advertising regulations in India were primarily governed by the Code for Self Regulation (**ASCI Code**) issued by the Advertising Standards Council of India (**ASCI**) which had limited statutory backing under the Cable Television Network Rules, 1994. However, the regulatory framework for advertising in India received a big boost with the issuance of the Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 under the Consumer Protection Act, 2019.

ASCI Code

The ASCI is a self-regulatory body of the Indian advertising industry. Its principal membership comprises advertisers, media, advertising agencies and other professional / ancillary service providers connected with advertising practices. ASCI has issued the ASCI Code, which requires advertisements to be "legal, decent, honest and truthful, and not hazardous or harmful, while observing fairness in competition".[1]

Although ASCI looks at advertisements across all media types and formats such as TV, print, digital, outdoor, radio, point of sale, etc. its legal backing comes from being notified under Rule 7 of the Cable Television Network Rules, 1994[2] which only govern advertisements on cable and satellite networks. There does not appear to be any statutory mechanism of enforcement of the ASCI Code in the digital realm.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (**Intermediary Rules**) which regulate the conduct of various intermediaries in India, require publishers of news and current affairs as well as online curated content to comply with the Programme Code under the Cable Television Networks (Regulation) Act, 1995,[3] however there is no such requirement to comply with the ASCI Code for advertising. It therefore appears that compliance with the ASCI Code in the digital realm is entirely voluntary. However since Facebook India Online Service Pvt. Ltd. as well as Google

[1] ASCI Annual Complaints Report 2022-23, available at https://www.ascionline.in/wp-content/uploads/2023/05/Complaints-Report-2022-23.pdf
[2] Rule 7(9), Cable Television Networks Rules, 1994.
[3] Appendix I, para (ii), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

India Pvt. Limited, are both members of ASCI as per its member information,[4] it would be useful to discuss the ASCI Code as both Google and Meta are significant players in the intermediary as well as the digital advertising sectors. Further, notwithstanding its lack of legal backing, it would be useful to understand the norms that the ASCI, as an industry body, has laid down for digital advertising.

The ASCI Code has general guidelines for its four basic or fundamental principles followed by guidelines for various specific categories of advertisements. The fundamental principles that the ASCI Code requires compliance with are:

(i) *Truthful and Honest Representation*: "To ensure the truthfulness and honesty of representations and claims made by advertisements, and to safeguard against misleading advertisements."

(ii) *Non-offensive to the public*: "To ensure that advertisements are not offensive to generally accepted standards of public decency."

(iii) *Against Harmful Products and Situations*: "To safeguard against the indiscriminate use of advertising for the promotion of products, which are regarded as hazardous to society or to individuals to a degree, or of a type which is unacceptable to society at large."

(iv) *Fair in Competition*: "To ensure that advertisements observe fairness in competition so that the consumer's need to be informed of choices in the marketplace and the canons of generally accepted competitive behavior in business is both served."

Regarding advertising in the digital world the ASCI Code has specific guidelines for (i) online gaming for real money, (ii) influencers in the digital media, (iii) advertising of virtual digital assets (more commonly known as cryptocurrencies) and linked services, and (iv) online deceptive design patterns (more commonly known as dark patterns). We shall now discuss these guidelines in greater detail:

(i) *Online gaming for real money*: Advertisers are required to ensure their advertisements are not depicting individuals under 18 playing such games and carrying a disclaimer about the addictive and financial risks. Advertisements should not promote gaming as an income opportunity or suggest unequal success among players. All gaming advertisements are required to include a disclaimer stating, "This game may be habit-forming or financially risky. Play responsibly." This disclaimer must occupy no less than 20% of the advertisement space and adhere to specific guidelines outlined in the ASCI Code. For audiovisual mediums, the disclaimer should be presented in both audio and visual formats, spoken at a normal pace at the end of the advertisement for a minimum of 4 seconds, and be in the same language as the advertisement. Importantly, the presentation of the disclaimer should be clear and free from any distractions caused by other actions, effects, claims, text, or audio.[5]

(ii) *Influencers in the digital media*: Disclosure is mandatory when a material connection exists between advertisers and influencers, extending beyond monetary compensation to any form of value exchanged. Even unbiased evaluations require disclosure if a material connection is present.

---

[4] https://www.ascionline.in/current-member/?category=digital-platforms

[5] ASCI Code, pg. 44, available at https://www.ascionline.in/wp-content/uploads/2024/04/Code-Book_Codes_Webready.pdf

However, if an influencer independently shares a product or service without a material connection, no disclosure is needed. The disclosure must be upfront and prominent, avoiding burying it among hashtags or links. Utilizing a platform's disclosure tool is recommended, and for picture or video posts without accompanying text, the disclosure label must be superimposed.[6]

(iii) *Virtual Digital Assets*: A mandatory disclaimer highlighting the unregulated and risky nature of crypto products and NFTs must be prominently displayed in various media formats, meeting specific size, duration, and language criteria. Guidelines emphasize prohibitions in including the use of terms like "currency," "securities," "custodian," and "depositories" in VDA advertisements. Advertisements should align with regulated entities' information and warnings, providing clear, accurate, and updated details on costs and profitability. Restrictions also apply to depicting minors, offering VDA products as a solution to problems, making profit guarantees, downplaying risks, or comparing VDAs to regulated asset classes. Celebrities in VDA ads must exercise due diligence to avoid misleading claims.[7]

(iv) *Dark Patterns*: The guidelines define dark patterns as business practices that impair consumer autonomy, decision-making, or choice through deceptive or manipulative elements in user interfaces, often aimed at increasing revenue. They cover practices such as drip pricing (hiding additional fees), bait and switch (misleading offers), false urgency (exaggerating limited availability), and disguised ads (not clearly disclosing sponsored content). These guidelines aim to ensure advertisements comply with Chapter 1 of the ASCI Code, which requires ads to be honest and not mislead consumers, and became applicable from September 1, 2023.[8]

The ASCI Guidelines prioritize transparency and clarity for consumers during influencer-promoted products or services on digital media and also aim to protect consumers and create consumer awareness in the unregulated VDA market. These Guidelines shape the media landscape that not only refrains from harmful stereotypes but also actively promotes positive and nuanced portrayals of gender in advertising.

Consumer Protection Act, 2019

The Consumer Protection Act, 2019 is perhaps the most important safeguard against misleading advertising that exists under Indian law. It defines the term misleading advertisement as follows:

> ""misleading advertisement" in relation to any product or service, means an advertisement, which—
>
> (i) falsely describes such product or service; or
>
> (ii) gives a false guarantee to, or is likely to mislead the consumers as to the nature, substance, quantity or quality of such product or service; or
>
> (iii) conveys an express or implied representation which, if made by the manufacturer or seller or service provider thereof, would constitute an unfair trade practice; or
>
> (iv) deliberately conceals important information;"[9]

[6] ASCI Code, pg. 46, available at https://www.ascionline.in/wp-content/uploads/2024/04/Code-Book_Codes_Webready.pdf
[7] ASCI Code, pg. 52, available at https://www.ascionline.in/wp-content/uploads/2024/04/Code-Book_Codes_Webready.pdf
[8] ASCI Code, pg. 60, available at https://www.ascionline.in/wp-content/uploads/2024/04/Code-Book_Codes_Webready.pdf
[9] Consumer Protection Act, 2019, Section 2(28).

The term advertisement has further been defined as follows:

> ""advertisement" means any audio or visual publicity, representation, endorsement or pronouncement made by means of light, sound, smoke, gas, print, electronic media, internet or website and includes any notice, circular, label, wrapper, invoice or such other documents;"[10]

Since the term advertisement includes electronic media, internet or website it would clearly cover digital advertisements as well. This means that all the safeguards under the Consumer Protection Act against misleading advertisements would apply fully to digital advertisements.

The Act establishes a Central Consumer Protection Authority which has the power to initiate actions relating to misleading advertisements and order discontinuance or modification of such advertisements and even impose a penalty if it deems appropriate to do so.[11] It also provides for imprisonment for misleading advertisements which are prejudicial to the interest of consumers.[12] In order to ensure that there is no false or misleading advertisement of any goods or services the Central Consumer Protection Authority has been given the power to issue guidelines for the protection of consumer interest[13] and it was in exercise of this power that the Authority has issued the (i) Guidelines for Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 ("**Advertisement Guidelines**"), and (ii) Guidelines for Prevention and Regulation of Dark Patterns, 2023 ("**Guidelines for Dark Patterns**").

Advertisement Guidelines

The Advertisement Guidelines are applicable to all advertisements regardless of form, manner or medium and are not only applicable to manufacturers and traders but also to advertising agencies which have been defined to include any person or establishment providing services of designing and production of advertisements or other related services for a commission or fees.[14] The Guidelines provide that unless an advertisement fulfils the following requirements it shall be considered a misleading advertisements:

> "(a) it contains truthful and honest representation;
>
> (b) it does not mislead consumers by exaggerating the accuracy, scientific validity or practical usefulness or capability or performance or service of the goods or product;
>
> (c) it does not present rights conferred on consumers by any law as a distinctive feature of advertiser's offer;
>
> (d) it does not suggest that the claims made in such advertisement are universally accepted if there is a significant division of informed or scientific opinion pertaining to such claims;
>
> (e) it does not mislead about the nature or extent of the risk to consumers' personal security, or that of their family if they fail to purchase the advertised goods, product or service;
>
> (f) it ensures that the claims that have not been independently substantiated but are based merely on the content of a publication do not mislead consumers;

---

[10] Consumer Protection Act, 2019, Section 2(1).
[11] Consumer Protection Act, 2019, Sections 19 and 21.
[12] Consumer Protection Act, 2019, Section 89.
[13] Consumer Protection Act, 2019, Section 18.
[14] Advertisement Guidelines, Para 2(c), available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf

(g) it complies with the provisions contained in any other sector specific law and the rules and regulations made thereunder."[15]

It also clarifies that the occasional and unintentional lapse in the fulfilment of the promise would not invalidate the advertisement provided that "(a) such promise or claim is capable of fulfilment by a typical specimen of the product advertised; (b) the proportion of product failures is within the generally acceptable limits; (c) the advertiser has taken prompt action to make good the deficiency to the consumer."[16]

The Guidelines lay down conditions for bait advertising i.e. where products are offered at a low price to attract customers. In such a scenario there has to be a reasonable prospect of selling such products at the price offered. The advertiser has to ensure that there is adequate supply to fulfil the foreseeable demand, and in case the advertiser believes there may not be enough supply then the advertiser has to state the reasonable grounds which the advertiser has for believing so. In particular the advertisement shall state clearly (i) that there is limited stock if the estimated demand exceeds the supply, (ii) whether the advertisement is for the purpose of assessing potential demand, and (iii) any restrictions including geographic and age-related restrictions on the availability of the product. Lastly the advertisement cannot mislead the consumers about the market conditions regarding the lack of availability of the product in order to induce the consumers to buy the products at less favourable conditions.[17]

Conditions have been imposed for advertising a product as "free" such as specifying that no product shall be described as free if the consumer has to pay for packaging, handling, administration, etc. or the cost of the accompanying product has been increased due to such promotion, or if the quality or quantity of the accompanying product has been reduced, etc.[18] Similarly the Guidelines impose a ban on surrogate advertising,[19] as well as advertising products which are either prohibited by law or prohibited from being advertised by any law.[20]

With respect to advertisements which target or use children, the Guidelines impose various conditions including conditions dealing with dangerous behaviour, physical and mental well-being, negative body image, prohibition on junk food and carbonated drinks being advertised during children's programming, etc.[21]

---

[15] Advertisement Guidelines, Para 4(1), available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf
[16] Advertisement Guidelines, Para 4(2), available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf
[17] Advertisement Guidelines, Para 5, available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf
[18] Advertisement Guidelines, Para 7, available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf
[19] Advertisement Guidelines, Para 6, available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf
[20] Advertisement Guidelines, Para 9, available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf
[21] Advertisement Guidelines, Para 8, available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf

The Guidelines also provide for a general obligation on all advertisers and advertising agencies to ensure that the claims in the advertisements are capable of substantiation, do not disrepute another person or institution without their consent, and should not contain statements or presentations that would mislead the consumers.[22] With regard to endorsements the Guidelines provide that any endorsement by a person or organisation about a product must be based on adequate information about, or experience with the product and any endorser who has a connection with the advertiser which might materially affect the credibility of the endorsement (and such connection may not be reasonably expected by the audience), such connection must be fully disclosed.[23] Additional guidelines for health influencers have also been issued by the Ministry to specifically deal with health and wellness celebrities, influencers and virtual influencers.[24]

Guidelines on Dark Patterns

In November, 2023 the CCPA issued Guidelines for the prevention and regulation of dark patterns in advertising. They defined the "dark patterns" as "any practices or deceptive design pattern using user interface or user experience interactions on any platform that is designed to mislead or trick users to do something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision making or choice, amounting to misleading advertisement or unfair trade practice or violation of consumer rights;"[25]

Unlike the Advertisement Guidelines, the Guidelines on Dark Patterns do not specifically refer to advertising agencies, but instead include (online) platforms within their scope. It may appear that the exclusion of advertising agencies might exclude significant players in the advertising technology arena such as Ad Exchanges, Ad Servers, SSPs, DSPs, etc. However, the wide definition of the term platform[26] would likely include all such stakeholders within its fold. The Guidelines provide that no person shall engage in any dark pattern practice and then specify that a person or platform shall be considered to be engaging in a dark pattern practice if it engages in any practice specified in Annexure 1 of the guidelines.[27] However the beginning of the Annexure clarifies that the dark pattern practices specified therein are only for guidance purposes and shall not be considered as a binding opinion or decision. These apparently contradictory provisions make the legal situation regarding specific dark pattern practices listed in the Annexure, somewhat ambivalent. That said, the Annexure lists the following as dark pattern practices:

(1) *False Urgency* i.e. falsely insinuating a sense of urgency so as to mislead the consumer into making an immediate purchase or into taking any other action which may lead to a purchase,

---

[22] Advertisement Guidelines, Para 12, available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf

[23] Advertisement Guidelines, Paras 13 and 14, available at https://consumeraffairs.nic.in/sites/default/files/CCPA_Notification.pdf

[24] https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Additional%20Influencer%20Guidelines%20for%20Health%20and%20Wellness%20Celebrities%2C%20Influencers%20and%20Virtual%20Influencers.pdf

[25] Guidelines on Dark Patterns, Para 2(1)(e), available at https://consumeraffairs.nic.in/sites/default/files/The%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%2C%202023.pdf

[26] The term platform has been defined as "an online interface in the form of any software including a website or a part thereof and applications including mobile applications;"

[27] Guidelines on Dark Patterns, Paras 4 and 5, available at https://consumeraffairs.nic.in/sites/default/files/The%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%2C%202023.pdf

"Illustrations:

(a) presenting false data on high demand without appropriate context. For instance, "Only 2 rooms left! 30 others are looking at this right now";

(b) falsely creating time-bound pressure to make a purchase, such as describing a sale as an 'exclusive' sale for a limited time only for a select group of users."

(2) *Basket Sneaking* i.e. including additional items such as services, payments to charity, etc. at the time of checkout, without the consent of the user, thereby increasing the total amount payable by the user;

"Illustrations:

(a) automatic addition of paid ancillary services with a pre-ticked box or otherwise to the cart when a consumer is purchasing a product or service;

(b) a user purchases a single salon service, but while checking out, a subscription to the salon service is automatically added;

(c) automatically adding travel insurance while a user purchases a flight ticket."

(3) *Confirm Shaming* i.e. creating a sense of fear or shame so as to nudge the consumer into purchasing a product or continuing a subscription.

"Illustrations:

(a) a platform for booking flight tickets using the phrase "I will stay unsecured", when a user does not include insurance in their cart;

(b) a platform that adds a charity in the basket without user's consent and uses a phrase such as "charity is for rich, I don't care" when a user prefers to opt out of contributing towards charity."

(4) *Forced Action* i.e. forcing a consumer into buying additional goods or subscriptions for unrelated services or sharing personal information, so that they can buy the product or service originally intended.

"Illustrations:

(a) prohibiting a user from continuing with the use of product or service for the consideration originally paid and contracted for, unless they upgrade for a higher rate or fees;

(b) forcing a user to subscribe to a newsletter in order to purchase a product;

(c) forcing a user to download an unintended or unrelated separate app to access a service originally advertised on another app e.g. A user downloads app, X, meant for listing houses for renting. Once the user downloads X, they are forced to download another app, Y, for hiring a painter. Without downloading Y, the user is unable to access any services on X;

(d) forcing a user to share personal information linked with Aadhar or credit card, even when such details are not necessary for making the intended purchase;

(e) forcing a user to share details of his contacts or social networks in order to access products or services purchased or intended to be purchased by the user;

(f) Making it difficult for consumers to understand and alter their privacy settings, thereby encouraging them to give more personal information than they mean to while making the intended purchase."

(5) *Subscription Trap* i.e. practices which make cancelling subscription impossible or complicated; or force a user to provide payment details or authorization to avail a free subscription; or make the cancellation instructions ambiguous or cumbersome, etc.

(6) *Interface Interference* i.e. designing the interface to highlight and obscure specific information in order to misdirect a user from taking an action as desired.

"Illustrations:

(a) designing a light colored option for selecting "No" in response to a pop-up asking a user if they wish to make a purchase or concealing the cancellation symbol in tiny font or changing the meaning of key symbols to mean the opposite;

(b) A 'X' icon on the top-right corner of a pop-up screen leading to opening-up of another advertisement rather than closing it;

(c) designing a virtually less prominent designing a light colored option for selecting "No" in response to a pop-up asking a user if they wish to make a purchase."

(7) *Bait and Switch* i.e. advertising a particular outcome based on the user's action but deceptively giving an alternate outcome.

"Illustrations:

(a) a seller offers a quality product at a cheap price but when the consumer is about to pay or buy, the seller states that the product is no longer available and instead offers a similar looking product but more expensive;

(b) a product is unavailable but is falsely shown as available to lure the consumer to move it to the shopping cart. Once the consumer moves it to the shopping cart, it is revealed that the product is 'out of stock' and instead, a higher-priced product is now available."

(8) *Drip Pricing* i.e. practices where elements of prices are not revealed upfront or products are advertised as free but continued usage would require in-app purchases, which is not disclosed; or preventing users from availing a service which is already paid for unless something additional is purchased.[28]

"*Illustrations*:

(a) A consumer is booking a flight, the online platform showcases the price as X at the checkout page, and when payment is being made, price Y (which is more than X) has been charged by the platform to the consumer;

(b) A consumer has downloaded a mobile application for playing chess, which was advertised as 'play chess for free'. However, after 7 days, the app asked for a payment to continue playing chess. The fact that the free version of the game is available only for a limited time, i.e., 7 days in this case, was not disclosed to the consumer at the time of downloading the mobile application;

(c) A consumer has purchased a gym membership. In order to actually use the gym, the user must purchase special shoes/boxing gloves from the gym, and the same was not displayed at the time of offering the gym membership."

(9) *Disguised Advertisement* i.e. masking advertisements as other kinds of content such as user content, news articles, etc. which are designed to blend in with the rest of an interface in order to trick customers.

(10) *Nagging* i.e. repeated and persistent interactions, in the form of requests, information, options, or interruptions, in order to effectuate a transaction.

"Illustrations:

(a) websites asking a user to download their app, again and again;

---

[28] However, a marketplace e-commerce entity would not be liable for price fluctuations to the extent attributable to price changes by third party sellers or due to other factors beyond their control.

(b) platforms asking users to give their phone numbers or other personal details for supposedly security purposes;

(c) constant request to turn on or accept notifications or cookies with no option to say "NO"."

(11) *Trick Question* i.e. the deliberate use of confusing or vague language such as double negatives, etc. in order to misguide a user.

"Illustrations:

(a) while giving a choice to opt, "Do you wish to opt out of receiving updates on our collection and discounts forever?" using phrases like, "Yes. I would like to receive updates" and "Not Now", instead of the option, "Yes"."

(12) *SaaS Billing* i.e. the process of generating and collecting payments from consumers on a recurring basis in a software as a service (SaaS) business model by exploiting positive acquisition loops in recurring subscriptions.

"Illustrations:

(a) no notification is given to the user when free trial is converted to paid;

(b) silent recurring transactions whereby the user's account is debited without being notified or simply stated auto-renewing monthly subscriptions without telling users;

(c) charging customers for features and services they don't use;

(d) using shady credit card authorization practices to deceive consumers."

(13) *Rogue Malware* i.e. using ransomware or scareware to mislead or trick users into believing there is a virus on their computer to convince them to pay for a fake malware removal tool that actually installs malware on their computer.

"Illustrations:

(a) when a pirating website/app promises the consumer to provide free content (audio or audio-visual or others) but actually leads to an imbedded malware when the link is accessed;

(b) when consumers gain access to the content on pirated platforms but keep getting pop-ups that have advertisements on them which are imbedded with malware;

(c) when consumers are prompted to click on an advertisement or are automatically redirected to an advertisement, but instead find their personal filed locked up, followed by a demand to make a payment to regain access."

The provisions of Consumer Protection Act apply to any violations of the Guidelines, and in such cases, the violators may be required to comply with relevant sanctions and directions by the authorities. Non-compliance with such directions may result in fines or imprisonment in one of two ways: (i) *through consumer complaints*: wherein the District Commission may order them to pay compensation for any loss or injury suffered by the consumer. Additionally they may be required to discontinue the unfair trade practice in question; (ii) *through the CCPA*: the CCPA has the power to investigate complaints relating to violation of consumer rights, unfair trade practices or misleading advertisements. Such an investigation can be initiated either on the CCPA's own motion, upon receiving a complaint or upon receiving a reference from the government.

Once the CCPA identifies a violation it may order the discontinuance of such practices and a failure to comply with such an order of the CCPA is punishable with imprisonment for a term which may extend to

six months or a fine of up to Rs. 20 lakhs or both. Further, giving false or misleading advertisements which are prejudicial to the interests of consumers would make the violators subject to criminal liability of imprisonment up to two years and a fine up to Rs. 10 lakhs for the first offence and imprisonment up to five years and fine up to Rs. 50 lakhs for subsequent offences.

Intermediary Guidelines

Rule 4(3) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 imposes a duty on significant social media intermediaries[29] to clearly mark any advertisements as information that is being advertised, marketed or sponsored, etc. Section 100 of the Consumer Protection Act, 2019 states that the provisions of the Act are in addition to and not in derogation of any other laws for the time being in force. Rule 3(1)(b)(xi) of the Intermediary Guidelines enjoins upon all intermediaries to make reasonable efforts to not host (directly or indirectly) information that violates any law, therefore it would appear that in case any advertisements violate any of the provisions under the Advertisement Guidelines or the Dark Pattern Guidelines, then any user may file a grievance with the intermediary to take down the advertisement as per the framework specified in the Intermediary Guidelines.

Other Jurisdictions

European Union

In Europe the new Digital Services Act[30] (**DSA**) of the European Union has provisions to prohibit dark patterns on online platforms. Apart from the DSA a number of other regulatory instruments also address dark pattern practices such as the General Data Protection Regulation[31] (**GDPR**), the Unfair Commercial Practices Directive[32] (**UCPD**), etc.

Article 25 of the DSA prohibits online platforms from designing their interfaces in a way that deceives or manipulates the users or materially distorts their ability to make free and informed decisions.[33] This would include exploitative design choices to direct users into acting in a way that benefits the platform, but which may not be in the users' interests, presenting choices in a non-neutral manner, such as giving more prominence to certain choices through visual, auditory, or other components.[34] It also empowers the Commission to issue guidelines on how this prohibition would apply to specific practices such as giving more prominence to certain choices, repeatedly asking users to make a choice, making cancellation more difficult than giving consent, etc.[35]

Online platforms are also required to inform their users that a particular information is an advertisement, the person on whose behalf the advertisement is presented and the person who paid for it. They are also

---

[29] Significant Social Media Intermediaries have been defined in section 2(1)(v) as "a social media intermediary having number of registered users in India above such threshold as notified by the Central Government"
[30] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[32] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:en:PDF
[33] DSA, Article 25(1), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
[34] Para 67 of the Preamble of DSA, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
[35] DSA, Article 25(2), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

required to provide the users easily accessible information about the parameters used to determine who the advertisement is presented to and how to change those parameters.[36]

In February 2023, the European Data Protection Board (EDPB) issued detailed guidelines on dark patterns (Guidelines) which offer practical recommendations on how to assess and avoid deceptive design patterns that infringe GDPR requirements, primarily the privacy principles given in Article 5.[37] The Guidelines various dark pattern practices such as overloading[38] (such as continuous prompting, privacy maze, too many options), skipping[39] (such as deceptive snugness, look over there), stirring[40] (emotional steering, hidden in plain sight), obstructing[41] (dead end, longer than necessary, misleading action), fickle[42] (lacking hierarchy, decontextualising, inconsistent interface, language discontinuity) and left in the dark[43] (conflicting information, ambiguous wording or information).

The European Commission has also issued a Guidance on the interpretation of the UCPD (**Guidance**) which, apart from a number of issues of online advertising, also addresses the issue of dark patterns.[44] Certain dark pattern practices such as "bait and switch", creating false urgency using fake timers or limited stock claims, inaccurate information on market conditions, falsely describing a product as free, nagging, etc. are already prohibited under Annex I to the UPCD.[45]

The Guidance further specifies that any business-to-consumer practice that materially distorts or is likely to distort the economic behaviour of an average or vulnerable consumer could breach the trader's professional diligence requirements amounting to a misleading practice or an aggressive practice prohibited under the UPCD, depending on the specific dark pattern applied, and there is no requirement of intention for the deployment of a dark pattern under the UPCD. Manipulative practices such as visually obscuring important information or ordering it in a way to promote a specific option or using trick questions or ambiguous language to confuse the user might qualify as misleading practices. While using emotion to steer users away from making a certain choice (such as 'confirm shaming') could amount to an aggressive practice.[46]

---

[36] DSA, Article 26(1), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065

[37] https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[38] Overloading means users are confronted with an avalanche/large quantity of requests, information, options or possibilities in order to prompt them to share more data or unintentionally allow personal data processing against the expectations of the data subject.

[39] Skipping means designing the interface or user journey in a way that users forget or do not think about all or some of the data protection aspects.

[40] Stirring affects the choice users would make by appealing to their emotions or using visual nudges.

[41] Obstructing means hindering or blocking users in their process of becoming informed or managing their data by making the action hard or impossible to achieve.

[42] Fickle means the design of the interface is inconsistent and not clear, making it hard for the user to navigate the different data protection control tools and to understand the purpose of the processing.

[43] Left in the dark means an interface is designed in a way to hide information or data protection control tools or to leave users unsure of how their data is processed and what kind of control they might have over it regarding the exercise of their rights.

[44] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)&from=EN

[45] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0022:0039:en:PDF

[46] Clause 4.2.7 of the Guidance, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1229(05)&from=EN

Regulators in other jurisdictions such as the Australian Competition and Consumer Commission[47] and the UK[48] have also been active in addressing the issue of dark patterns practices.

Australia

The Australian Association of National Advertisers (AANA) Code of Ethics also plays a pivotal role in regulating advertising practices, ensuring ethical standards are upheld within the industry. Advertisers are mandated to adhere to specific provisions outlined in the Code to maintain transparency and protect consumers. Compliance with laws,[49] necessitates adherence to both Commonwealth and relevant State or Territory laws, safeguarding against illegal advertising practices. Avoidance of misleading advertising requires advertisers to refrain from engaging in deceptive practices, emphasizing transparency and consumer protection.[50] It also underscores the importance of competitor integrity, urging advertisers to promote fair competition and abstain from making detrimental misrepresentations against competitors.[51] Advertisers are also urged to exercise environmental responsibility by ensuring truthful environmental claims and avoiding misleading exploitation of community concerns.[52] Moreover, provision 1.5 emphasizes the necessity of accurate Australian origin claims in advertisements to foster consumer trust and transparency.[53] Additionally, regarding content and portrayal, the Code of Ethics highlights the significance of non-discrimination, responsible use of sexual appeal, and portrayal of violence in advertising.[54] Non-compliance with these guidelines can lead to significant consequences for advertisers impacting reputation and legal ramifications affecting company liabilities.

---

47 https://sharongivoni.com.au/dark-patterns-user-interfaces-that-make-consumers-buy-and-buy-more-what-are-the-laws-and-are-dark-patterns-illegal/#:~:text=The%20Australian%20Consumer%20Law%20(ACL,to%20mislead%20or%20deceive%20consumers

48 https://www.drcf.org.uk/publications/papers/ico-cma-joint-paper-on-harmful-design-in-digital-practices

49 Provision 1.1, https://f.hubspotusercontent00.net/hubfs/5093205/AANA_Code_of_Ethics_Effective_February_2021.pdf?utm_campaign=Self-Reg-Codes&utm_source=AANA&utm_medium=web&utm_term=self-reg&utm_content=code-of-ethics

50 Provision 1.2, https://f.hubspotusercontent00.net/hubfs/5093205/AANA_Code_of_Ethics_Effective_February_2021.pdf?utm_campaign=Self-Reg-Codes&utm_source=AANA&utm_medium=web&utm_term=self-reg&utm_content=code-of-ethics

51 Provision 1.3, https://f.hubspotusercontent00.net/hubfs/5093205/AANA_Code_of_Ethics_Effective_February_2021.pdf?utm_campaign=Self-Reg-Codes&utm_source=AANA&utm_medium=web&utm_term=self-reg&utm_content=code-of-ethics

52 Provision 1.4, https://f.hubspotusercontent00.net/hubfs/5093205/AANA_Code_of_Ethics_Effective_February_2021.pdf?utm_campaign=Self-Reg-Codes&utm_source=AANA&utm_medium=web&utm_term=self-reg&utm_content=code-of-ethics

53 https://f.hubspotusercontent00.net/hubfs/5093205/AANA_Code_of_Ethics_Effective_February_2021.pdf?utm_campaign=Self-Reg-Codes&utm_source=AANA&utm_medium=web&utm_term=self-reg&utm_content=code-of-ethics

54 https://f.hubspotusercontent00.net/hubfs/5093205/AANA_Code_of_Ethics_Effective_February_2021.pdf?utm_campaign=Self-Reg-Codes&utm_source=AANA&utm_medium=web&utm_term=self-reg&utm_content=code-of-ethics

Although there is no law specifically governing dark patterns in Australia yet, the Treasury, Government of Australia[55] as well as the Australian Competition and Consumer Commission[56] have both come out with reports discussing the effects of dark patterns on consumer choices and their rights.

Singapore

The Singapore Code of Advertising Practice (SCAP) is a comprehensive set of guidelines that govern advertising practices in Singapore across various mediums. These regulations cover a wide range of advertising formats to ensure ethical standards are maintained in the industry. Specifically, the SCAP applies to all advertisements for goods, services, and facilities, regardless of their origin, and includes but is not limited to:[57]

- Advertisements in newspapers, magazines, brochures, leaflets, circulars, mailings, posters, and other printed publications;
- Advertisements via facsimile transmissions and aerial announcements;
- Advertisements displayed on buildings and vehicles;
- Television, radio, cinema, and video commercials;
- Advertisements in information network services, electronic bulletin boards, online databases, and Internet services;
- Advertisements in non-broadcast electronic media such as computer games;
- Mail orders, sales promotions, and mailing lists;
- Digital communications in every format, design, and context including the world-wide web (Internet);
- Telephone advertising.

These regulations ensure that advertisements are legal, decent, honest, and truthful, prepared with a sense of responsibility to consumers and society, and conform to the principles of fair competition.[58] Advertisements are also expected to uphold Singapore's shared values and family values, avoiding practices that could bring advertising into disrepute or reduce confidence in it as a service to industry and the public. The SCAP aims to protect the rights of consumers and maintain high ethical standards in advertising practices throughout various media channels.

Concluding Remarks

Advertising guidelines for traditional media have traditionally had conditions to ensure there is no misrepresentation in advertisements and that there are no harmful effects from the advertising itself. However when dealing with digital advertising it was clear that the traditional framework was not enough which is why a need was felt to supplement the existing framework with provisions specifically dealing with digital advertising. As a result of this, steps have been taken in various jurisdictions such as the European Union as well as India to specifically identify and prohibit harmful practices in digital advertising such as drip pricing, bait and switch, nagging, etc. usually referred to as Dark Patterns.

---

[55] https://treasury.gov.au/sites/default/files/2023-08/c2023-430458-cris1.pdf
[56] https://www.accc.gov.au/system/files/Digital%20advertising%20services%20inquiry%20-%20final%20report.pdf
[57] https://asas.org.sg/Portals/0/SCAP%202008_1.pdf
[58] https://asas.org.sg/Portals/0/SCAP%202008_1.pdf

While the identification and prohibition of such practices by regulators is an important and encouraging first step, a lot would depend upon effective enforcement of these provisions by the regulators.

DATA PROTECTION

Data protection is a critical issue for digital advertising as the business model of digital advertising revolves around the collection, storage, and use of personal data from consumers. Advertisers rely heavily on user data to target ads effectively, but there are growing concerns over privacy violations and the misuse of sensitive information. Regulations like the General Data Protection Regulation (GDPR) in the European Union have aimed to give users more control over their data and impose strict rules on how companies handle personal information. Striking the right balance between personalized advertising and data privacy is a major challenge for the industry, as companies must navigate complex legal requirements while also maintaining consumer trust and avoiding backlash over intrusive data practices.

Indian Law

India did not have a dedicated data protection law till 2023 and the legal framework before 2023 consisted primarily of the Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011 backed up by judicial pronouncements, both of which were limited in scope. This situation has recently undergone a significant change with the passage of the Digital Personal Data Protection Act, 2023.

Digital Personal Data Protection Act, 2023

In August of 2023, the Parliament of India passed the long awaited data protection legislation in the form of the Digital Personal Data Protection Act, 2023 (**DPDPA**). Although the DPDPA is a much trimmed down version as compared to previous versions that were under discussion,[59] it is a significant improvement on the existing framework for data protection which was primarily governed by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. It recognises the citizens' right to consent, to correction and erasure, to grievance redressal, and to nominate a representative in the event of incapacity. It also outlines the obligations of Significant Data Fiduciaries (SDFs), a classification based, *inter alia*, on volume and sensitivity of the data handled. There is however significant room for improvement in the DPDPA such as changes to the Data Protection Board of India, etc.

Much like the General Data Protection Regulations of the EU, the DPDPA is extra territorial in nature i.e. it is also applicable to data processing outside of India, if such processing is in connection with any activity related to offering of goods or services within the territory of India.[60] It defines the term personal data as "any data about an individual who is identifiable by or in relation to such data".[61] Although the definition includes data in relation to which an individual is identifiable, it is not clear if it would include such data which by itself does not identify an individual but which in conjugation with other data is capable of identifying an individual. Central government has been given the power to specify State instrumentalities who may process data without application of the provisions of the Act. The provisions of the DPDPA shall also not be applicable for processing that is necessary for research, archiving or

[59] See the Personal Data Protection Bill, 2018, available at https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
[60] Digital Personal Data Protection Act, 2023, Section 3(b).
[61] Digital Personal Data Protection Act, 2023, Section 2(t).

statistical purposes if certain other conditions are satisfied.[62] The Act also provides for certain other circumstances under which specific provisions of the DPDPA do not apply to specified data fiduciaries.[63]

The DPDPA bans the collection and processing of personal data except where done in accordance with the provisions of the DPDPA and for which the data principal has given specific consent[64] which shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action and be limited to only such personal data as is necessary for the specified purpose.[65] When dealing with the concept of data necessary for the specified purpose, Illustration under section 6(1) is quite significant, its states as follows:

> "X, an individual, downloads Y, a telemedicine app. Y requests the consent of X for (i) the processing of her personal data for making available telemedicine services, and (ii) accessing her mobile phone contact list, and X signifies her consent to both. Since phone contact list is not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services."

The data principal has also been given the right to withdraw her consent at any time and it is specified that the ease of withdrawing consent shall be comparable to the ease with which such consent was given.[66] The data principal may also appoint a consent manager to act as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Every consent manager shall be registered with the Data Protection Board of India and be accountable to the data principal and act on her behalf in the manner and subject to the conditions as may be prescribed.[67]

The Act specifies the obligations and responsibilities of a data fiduciary such as implementing appropriate technical and organisational measures to ensure compliance with the DPDPA, taking reasonable security safeguards to prevent personal data breach, notify the Board and the data principal of a personal data breach, erasing personal data upon withdrawal of consent, establishment of a grievance redressal mechanism, etc.[68] Data fiduciaries are prohibited from processing personal data of children if it is likely to cause a detrimental effect on the wellbeing of the child, tracking or behavioural monitoring of children or targeted advertising directed at children, unless the data fiduciary is specifically allowed to do so by Rules or notification.[69]

The data principal is granted certain rights under the DPDPA such as obtaining certain information from the data fiduciary regarding the processing activities undertaken on the personal data, identities of all data processors with whom the data has been shared as well as any other information that has been prescribed.[70] The data principal also has the right to correction, completion, updating or erasure of the

---

[62] Digital Personal Data Protection Act, 2023, Section 17(2).
[63] Digital Personal Data Protection Act, 2023, Section 17(3), (4) and (5).
[64] Digital Personal Data Protection Act, 2023, Section 4.
[65] Digital Personal Data Protection Act, 2023, Section 6(1).
[66] Digital Personal Data Protection Act, 2023, Section 6(4).
[67] Digital Personal Data Protection Act, 2023, Section 6(7), (8) and (9).
[68] Digital Personal Data Protection Act, 2023, Section 8.
[69] Digital Personal Data Protection Act, 2023, Section 9.
[70] Digital Personal Data Protection Act, 2023, Section 11.

personal data,[71] to a readily available grievance redressal mechanism,[72] and to nominate an individual to exercise the rights of the data principal in case of death or incapacity.[73] These rights also come along with obligations that the data principal has to comply with such as not to impersonate another person while providing personal data, not to file false or frivolous complaints, furnishing only verifiable authentic information when exercising the right to correction or erasure, etc.[74]

The DPDPA creates a special category of significant data fiduciaries which will be notified by the Central Government, based upon the volume and sensitivity of the data processed, risks to the data principal, potential impact on the sovereignty and integrity of India, etc. Significant data fiduciaries have to appoint a Data Protection Officer who shall be based in India and report to the upper management, appoint an independent data auditor and also undertake periodic data protection impact assessments, periodic audits and such other measures as may be prescribed in this regard.[75]

The DPDPA establishes a Data Protection Board of India[76] which is envisaged as a quasi-judicial body with powers such as directing remedial and mitigation measures in case of a data breach, inquiring into non-compliance by data fiduciaries and consent managers of their obligations and impose penalties, inquiring into breach of blocking orders issued under section 37 by intermediaries and impose penalties.[77]

Other Jurisdictions

Europe

In April of 2016 the European Council and Parliament approved the General Data Protection Regulation (**GDPR**), which came into effect on May 25, 2018 replacing the old data protection regime which was in place by virtue of the Data Protection Directive of 1995 (**DPD**). The earlier regime through the DPD was merely a directive which required member states to pass their own legislations which were to be in line with the DPD, however the GDPR is a regulation which means that it would have direct legal effect throughout the European Union without any need for national legislations.[78] The scope of the GDPR is not limited merely to the territory of the European Union but also applies to processing of data outside of the European Union, as long as it is personal data of persons residing in the European Union.[79] It even applies to data controllers or data processors established outside the EU if their activities relate to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[80]

---

[71] Digital Personal Data Protection Act, 2023, Section 12.
[72] Digital Personal Data Protection Act, 2023, Section 13.
[73] Digital Personal Data Protection Act, 2023, Section 14. The rights of the data principal under sections 11 to 15 shall not apply in case of the exemptions specified under section 17(1).
[74] Digital Personal Data Protection Act, 2023, Section 15.
[75] Digital Personal Data Protection Act, 2023, Section 10.
[76] The Data Protection Board of India is yet to be formally set up.
[77] Digital Personal Data Protection Act, 2023, Section 27.
[78] https://www.sgrlaw.com/a-primer-on-the-eus-general-data-protection-regulation/
[79] General Data Protection Regulation, Article 3(1), available at https://gdpr-info.eu/
[80] General Data Protection Regulation, Article 3(2), available at https://gdpr-info.eu/

The GDPR requires data controllers and processors whose activities require regular and systematic monitoring on a large scale or who process special types of data, to appoint a Data Protection Officer who should have expertise in data protection law and practices.[81] It requires that data should be processed in accordance with the following privacy principles:[82]

(i) Lawfulness, fairness and transparency – data processing must be done in a lawful, fair and transparency manner in relation to the data subject;
(ii) Purpose limitation – data should be collected and processed only for explicit and legitimate purposes and no further processing should occur that is incompatible with those purposes;
(iii) Data minimisation – only such data that is adequate and relevant for the purpose of collection should be collected and processed;
(iv) Accuracy – data must be kept accurate and (where necessary) up to date;
(v) Storage limitation – data should be kept in a form that could identify the data subject only for as long as is necessary for the purpose for which it was collected;
(vi) Integrity and confidentiality – data should be processed in a manner that ensures appropriate security;
(vii) Accountability – the data controller should be able to demonstrate compliance with the data principles given above.[83]

Apart from the above broad principles specific provisions have been made to deal with important issues such as conditions for consent, breach notifications, right to be forgotten, etc. which are enumerated below in brief:

Conditions for Consent

The GDPR provides that consent must be given in an intelligible and easily accessible form using clear and plain language and in case it is taken in a written declaration that also contains other matters, then the request for consent has to be clearly distinguishable from the other matters. In order to assess whether consent is freely given, utmost consideration is to be given to whether the performance of the contract or provision of the service is conditional on the consent to processing of personal data which is not essential to the performance of the contract or provision of service. The GDPR also provides the data subject with the right to withdraw the consent and also specifies that it should be as easy to withdraw the consent as it was to give the consent in the first place.[84]

Breach Notification

All data controllers and data processers are required to notify the data subjects of a personal data breach without undue delay in case the breach is likely to result in high risk to the rights and freedoms of natural persons, unless measures have been taken to (i) make it unintelligible to any unauthorised person (such as encryption), (ii) ensure that the risk to the rights and freedoms is no longer likely to materialise, or (iii) it would involve disproportionate effort, in which case a public communication would be made. In case the

[81] General Data Protection Regulation, Article 37, available at https://gdpr-info.eu/
[82] General Data Protection Regulation, Article 5, available at https://gdpr-info.eu/
[83] The Guidelines of the EBDP on how these principles would be violated by Dark Patterns in online Advertising are given above.
[84] General Data Protection Regulation, Article 7, available at https://gdpr-info.eu/

personal data breach is not likely to result in a high risk to the rights and freedoms of natural persons, the data controller is required to notify the supervisory authority of the data breach, where feasible, within 72 hours.[85]

Right to be Forgotten

The GDPR specifically recognises a person's right to be forgotten (or right to erasure) which entitles a person to get the data controller to erase the person's personal data without undue delay if (a) there is withdrawal of consent, (b) the data is no longer necessary for the purpose for which it was collected, (c) the person objects to the data being processed on the grounds listed in Article 21, or (d) the data was unlawfully processed, etc. It must be noted that the right to be forgotten is not an absolute right, i.e. a mere request for erasure of the data is not enough to ensure compliance by the data controller; once a request is made the data controller has to evaluate it and may deny the request if it determines that it is necessary (a) for exercising the right to freedom of expression and information, (b) for compliance with a legal obligation, or (c) for reasons of public interest in the area of public health (as per Article 9(2)(h) and (i)), (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, (e) for the purpose of exercising or defending legal claims.[86]

Data Protection by Design

Data controllers have an obligation to implement appropriate technical and organisational measures (such as pseudonymisation), both at the stage of design and at the time of processing itself, which take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood, which are designed to implement the data protection principles. The data controllers also have to ensure that by default, only personal data which is necessary for each specific purpose of the processing is processed.[87]

Right to Access

The GDPR also gives the right to a person to get a confirmation from the data controller as to whether or not their personal data is being processed or not. In case the data is being processed the person also has the right to obtain information regarding the (a) the purposes of the processing, (b) the categories of personal data, (c) the recipients or categories of recipient to whom the personal data is disclosed, (d) the existence of the right to request rectification or erasure, (e) the right to lodge a complaint with a supervisory authority; (f) where the personal data is not collected from the data subject, any available information as to its source; (g) the existence of automated decision-making, including profiling, etc.

Australia

In Australia data protection is governed primarily by the Privacy Act 1988[88] as amended from time to time and the Australian Privacy Principles[89] with the Privacy Commissioner who sits within the Office of the Australian Information Commissioner being the relevant regulator for data protection, responsible for

[85] General Data Protection Regulation, Articles 33 and 34, available at https://gdpr-info.eu/
[86] General Data Protection Regulation, Article 17, available at https://gdpr-info.eu/
[87] General Data Protection Regulation, Article 25, available at https://gdpr-info.eu/
[88] https://www.dataguidance.com/legal-research/privacy-act-1988-no-119-1988-amended
[89] https://www.dataguidance.com/legal-research/australian-privacy-principles-2014

the enforcement of the Privacy Act. The Privacy Act regulates the collection, use, holding and disclosure of the personal information of living individuals and although there is no defined concept of a data controller or data processor in Australian law, each entity that obtains or receives personal data (usually referred to as APP entities) has its own set of obligations under Australian privacy laws.[90] Personal information is defined as "information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not".

The Australian Privacy Principles given in the Schedule of the Privacy Act basically govern the standards, rights and obligations around the collection, use and disclosure of personal information. A brief summary of the principles is given below:[91]

(i) *Open and transparent management of personal information* - Ensures that APP entities manage personal information in an open and transparent way such as having a clear privacy policy, etc.
(ii) *Anonymity and pseudonymity* - APP entities have to give individuals, with some exceptions, the option of not identifying themselves, or of using a pseudonym.
(iii) *Collection of solicited personal information* - Specifies when an APP entity can collect personal information that is solicited and contains higher standards when dealing with the collection of 'sensitive' information.
(iv) *Dealing with unsolicited personal information* - Deals with how APP entities must deal with unsolicited personal information.
(v) *Notification of the collection of personal information* - Specifies the circumstances in which an APP entity that collects personal information is required to notify an individual of certain matters.
(vi) *Use or disclosure of personal information* - Specifies the circumstances under which personal information may be disclosed.
(vii) *Direct marketing* - This principle specifies that an organisation may use or disclose personal information for direct marketing purposes only if certain specific conditions are met.
(viii) *Cross-border disclosure of personal information* - Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
(ix) *Adoption, use or disclosure of government related identifiers* - Specifies the circumstances under which an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.
(x) *Quality of personal information* - Requires APP entities to take reasonable steps to ensure the personal information they collect, use or disclose is accurate, up to date and complete.
(xi) *Security of personal information* - Requires APP entities to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
(xii) *Access to personal information* - Contains an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity.
(xiii) *Correction of personal information* - Specifies APP entities' obligations in relation to correcting the personal information they hold about individuals.

---

[90] https://www.dataguidance.com/notes/australia-data-protection-overview
[91] Office of the Australian Information Commissioner, "Australian Privacy Principles Quick Reference", https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference

It must be noted that personal information which is not sensitive information (or other restricted information) and which is reasonably necessary for the APP entity's functions or activities can be collected directly from the individual after providing an appropriate notice (such as a privacy statement or policy) at or prior to collection. However for the collection of sensitive information consent (express or implied) is required. Even with consent the sensitive information can only be collected if it is also reasonably necessary for one or more of the APP entity's functions or activities.[92]

Singapore

The primary data protection legislation in Singapore is the Personal Data Protection Act, 2012 and various Regulations issued under it. The Personal Data Protection Commission under the Infocomm Media Development Authority of Singapore (**IMDA**) is the authority responsible for administering and enforcing the Act. It defines personal data as data, whether true or not, about an individual who can be identified: (a) from that data; or (b) from that data and other information to which the organisation is likely to have access. The Act requires that consent of an individual (express or deemed) must be obtained before collecting, using or disclosing personal data for any purpose. Certain exceptions to this consent requirement are provided in the First or Second Schedule to the Act.[93] The Act also gives the individual the right to withdraw the consent, upon which the organisation must stop collecting, using or disclosing the data.[94] It also provides that the organisation collecting the data must notify individuals about the purpose for which it intends to collect, use or disclose the personal data before such collection, use or disclosure.[95] Organisations are required to appoint data protection officers and also develop and implement policies and procedures necessary to ensure implementation of the Act, which policies must be publicly available.[96] The Act provides that an organisation can collect, use or disclose personal data only for purposes that a reasonable person would consider appropriate in the circumstances.[97] It requires organisations to ensure that the data collected is accurate and complete if it is likely to be used to make a decision that affects the individual to whom the data relates.[98] Further organisations are required to make reasonable security and data protection arrangements in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, etc. of the data.[99]

The Act gives the individual the right to request an organisation to allow access to the individual's personal data as well as the ways in which the data has been used or may have been used or disclosed.[100] The individual also has the right to request correction of an error or omission in the personal data.[101]

---

[92] https://www.dataguidance.com/notes/australia-data-protection-overview
[93] Personal Data Protection Act, 2012, Sections 13 to 17.
[94] Personal Data Protection Act, 2012, Section 16.
[95] Personal Data Protection Act, 2012, Section 20.
[96] Personal Data Protection Act, 2012, Sections 11 and 12.
[97] Personal Data Protection Act, 2012, Section 18.
[98] Personal Data Protection Act, 2012, Section 23.
[99] Personal Data Protection Act, 2012, Section 24.
[100] Personal Data Protection Act, 2012, Section 21.
[101] Personal Data Protection Act, 2012, Section 22.

Although not specifically provided in the Act, the PDPC advises that as a best practice, organisations should avoid over collecting personal data where this is not required for their business or legal purposes.[102]

Concluding Remarks

The recent flurry of data protection legislations in major jurisdictions, led by the EU's GDPR are expected to force major changes in the digital advertising industry. One of the main issues that would drive this change are the requirements for explicit consent before any data is collected. Most legislations require that before any data is collected the explicit (as opposed to implicit) consent of the data subject is to be taken. They also provide that the notice asking for consent must be given in easy to read and understand language without the use of unnecessary legalese. Such a provision would severely impact web pages that load data collecting ad scripts before any consent of the user is obtained and would force publishers to rethink the timing and placement of advertisements and scripts on their homepage, which is their most valuable advertising real estate.[103] A big page asking for consent before loading the homepage runs the risk of driving away traffic, thereby causing loss to the publishers. On the upside publishers and news media websites are more likely to be granted such consent by data subjects as opposed to ad platforms and networks, thereby placing them back in a favourable position compared to such advertising intermediaries. Perhaps the entities that would be most adversely affected would be the third-party ad networks that are not already part of one of the large platform companies (e.g., Google, Facebook, Amazon). These smaller ad networks which typically lack the direct consumer relationships needed to secure consent from users may also find that media publishers and other website hosts are reluctant to ask for user consent for the broad range and volume of data that these advertisers need for effective operations. Without access to the data such networks may be simply cut out of the online market altogether.[104]

Legal mandates that require explicit consent before collecting and processing any personal data put the burden of obtaining consent on marketers and under the GDPR, individuals must opt-in before receiving marketing communications. These circumstances have demolished the mass email marketing option for digital marketers.[105]

The legislations also require that only such personal data as is necessary for the specified purpose must be collected, for eg. a telemedicine app on a smartphone does not need access to a user's contact list since it is not necessary for the purpose of availing telemedicine services. In such cases even if the data subject gives explicit consent for accessing the contact list, such consent will not be considered valid and would be limited only to the processing of personal data for telemedicine services.

[102] https://www.pdpc.gov.sg/news-and-events/press-room/2015/05/avoid-overcollection-of-personal-data
[103] https://www.cjr.org/tow_center_reports/understanding-general-data-protection-regulation.php
[104] https://www.cjr.org/tow_center_reports/understanding-general-data-protection-regulation.php
[105] https://tsaaro.com/blogs/the-impact-of-gdpr-on-digital-marketing-a-marketer-s-guide-to-compliance/

COMPETITION LAW

The purpose of competition law is to prevent anti-competitive practices that harm consumer welfare. The issue of competition law in the digital advertising sector has become increasingly prominent as a few major tech companies dominate the landscape, raising concerns about market power and anti-competitive practices. The business model of digital advertising is characterized by its complex, data-driven nature and rapid technological advancements. Ensuring a fair and competitive market is essential not only for fostering innovation but also for protecting consumers and smaller businesses from potential abuses of power. As such, regulatory bodies are actively exploring new frameworks and enforcement mechanisms to address these challenges in an evolving digital economy.

Indian Law

Unlike the regulatory landscape for consumer advertising the competition law framework of India comprises entirely of a single legislation, viz. the Competition Act, 2002 under which the Competition Commission of India (CCI) is responsible for ensuring anti-competitive practices in India.

Competition Act, 2002

The Competition Act, 2002, prohibits both antitrust agreements[106] as well as abuse of dominance.[107] It also regulates combinations (mergers, acquisitions, etc.) above a certain threshold and any combinations which breach the threshold require prior approval from the CCI, else they would be void.[108] Section 3 of the Competition Act prohibits any agreements in respect of production, supply, distribution, storage, acquisition or control of goods or provision of services, which causes or is likely to cause an appreciable adverse effect on competition within India and declares that any such agreements would be void. It further specifies certain types of agreements[109] which will be deemed to have an appreciable adverse effect on competition, and thus deemed void. The Act also specifies certain other factors that have to be taken into account in order to determine if an agreement has an appreciable adverse effect on competition, namely:

> "(a) creation of barriers to new entrants in the market;
> (b) driving existing competitors out of the market;
> (c) foreclosure of competition by hindering entry into the market;
> (d)accrual of benefits to consumers;
> (e) improvements in production or distribution of goods or provision of services; or

[106] Competition Act, 2002, Section 3.
[107] Competition Act, 2002, Section 4.
[108] Competition Act, 2002, Sections 5 and 6.
[109] Competition Act, 2002, Section 3(3) - Any agreement which "(a) directly or indirectly determines purchase or sale prices; (b) limits or controls production, supply, markets, technical development, investment or provision of services; (c) shares the market or source of production or provision of services by way of allocation of geographical area of market, or type of goods or services, or number of customers in the market or any other similar way; (d) directly or indirectly results in bid rigging or collusive bidding,". Section 3(4) - Any agreement "amongst enterprises or persons at different stages or levels of the production chain in different markets, in respect of production, supply, distribution, storage, sale or price of, or trade in goods or provision of services, including— (6) (a) tie-in arrangement; (b) exclusive supply agreement; (c) exclusive distribution agreement; (d) refusal to deal; (e) resale price maintenance."

(f) promotion of technical, scientific and economic development by means of production or distribution of goods or provision of services"[110]

Section 4 of the Act prohibits a dominant enterprise in the relevant market from abusing its dominant position and specifies the factors that are to be considered in determining whether an enterprise enjoys a dominant position. It must be pointed out that the Act does not seek to prohibit the dominance of an enterprise *per se* but only the abuse of such dominant position by an enterprise,[111] and lists out certain practices which would constitute an abuse of dominant position, such as if the group or enterprise:

"(a) directly or indirectly, imposes unfair or discriminatory—

(i) condition in purchase or sale of goods or service; or

(ii) price in purchase or sale (including predatory price) of goods or service; or

Explanation.— For the purposes of this clause, the unfair or discriminatory condition in purchase or sale of goods or service referred to in sub-clause (i) and unfair or discriminatory price in purchase or sale of goods (including predatory price) or service referred to in sub-clause (ii) shall not include such discriminatory condition or price which may be adopted to meet the competition; or

(b) limits or restricts—

(i) production of goods or provision of services or market therefor; or

(ii) technical or scientific development relating to goods or services to the prejudice of consumers; or

(c) indulges in practice or practices resulting in denial of market access in any manner; or

(d) makes conclusion of contracts subject to acceptance by other parties of supplementary obligations which, by their nature or according to commercial usage, have no connection with the subject of such contracts; or

(e) uses its dominant position in one relevant market to enter into, or protect, other relevant market."[112]

Although the Act adopts an *ex ante* stance when it comes to combinations, it has an *ex post* approach when dealing with antitrust agreements and abuse of dominant position.

The Competition Law Review Committee (CLRC) set up by the Ministry of Corporate Affairs had in its 2019 Report[113] suggested that the scope of section 3 of the Competition Act should be increased in order to comprehensively cover all kinds of anti-competitive restraints and agreements, specially those pertinent to digital markets and recommended including the term 'other agreements' under section 3(4) of the Competition Act so as to enlarge its scope. This recommendation was accepted and implemented through the Competition (Amendment) Act, 2023.

CLRC had also pointed out that the acquisition of smaller successful start-ups by dominant firms in the digital space tends to escape regulatory scrutiny because they often do not meet the asset and turnover-based thresholds provided under the Competition Act and the CCI does not have any power to

[110] Competition Act, 2002, Section 19(3).
[111] Competition Act, 2002, Section 4(1).
[112] Competition Act, 2002, Section 4(2).
[113] https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf, pg. 63.

assess transactions which are not required to be notified. To address this problem the CLRC Report had recommended the introduction of new thresholds based on broad parameters for merger notification under the Competition Act.[114] This suggestion was also accepted in the Competition (Amendment) Act, 2023 which introduced a deal value threshold of Rupees 2,000 crore for notifying a transaction to the CCI if the entity being acquired has 'substantial business operations' in India.[115] The Competition (Amendment) Act, 2023 has also expanded the scope of 'relevant market' under sections 19(6) and 19(7) of the Competition Act by specifying factors such as the nature of services and costs associated with switching demand or supply.

Proceedings before the CCI

Under the Competition Act, 2002 enforcement actions occur in stages starting with the formation of a *prima facie* view by the CCI,[116] followed by an investigation by the Director General[117] and if necessary an enquiry by the DG or the CCI itself.[118] After considering the various reports and hearing the enterprise being proceeded against, the CCI passes a final order.[119] In terms of the market for online advertising, there have been two significant cases before the CCI, both involving Google, one filed by a matrimonial website and the other by a news publishers' association. A brief summary of both these proceedings is given below, which would give an illustration of how the existing regulations in India have been tried to be used to curb anti competitive practices in India. It is to be noted that while the CCI orders in these cases dealt with multiple issues, we are only discussing the allegation of anti competitive practices relating to online advertising services.

Digital News Publishers Association Case[120]

In this case the CCI has only issued a *prima facie* opinion and asked the DG to investigate the alleged violations of section 4 by Google in payments made by it to news publishers. The CCI, has *prima facie* held not only that Google is dominant in the relevant market for online search advertising services in India but occupies a significant position in the market for online digital advertising intermediation services as well.[121] The CCI also stated that "it appears that the instant information highlights the alleged bargaining power imbalance that flows from the alleged position enjoyed by Google as a necessary trading partner for digital news publishers in accessing online audience as well as in generating digital ad revenue. The case also brings forth the issue of alleged lack of transparency and information asymmetry in the ad tech services provided by Google, which does not allow publishers to optimize the yield on their ad inventory."[122]

[114] https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf, pg. 133.
[115] Competition Act, 2002, Section 5(d).
[116] Competition Act, 2002, Section 26(1).
[117] Competition Act, 2002, Section 26(3).
[118] Competition Act, 2002, Section 26(7) and (8).
[119] Competition Act, 2002, Section 27.
[120] Case No. 41 of 2021, dated 07-01-2022, available at https://www.cci.gov.in/antitrust/orders/details/11/0
[121] Digital News Publishers Association Case, paras 21 and 32.
[122] Digital News Publishers Association Case, para 22.

It was brought out that news publishers are heavily dependent on Google for a majority of their traffic and they have little choice but to accept the terms and conditions imposed by Google which also operates as a gateway between various news publishers on the one hand and news readers on the other. It was claimed by the news publishers association that the terms of the agreements entered between the members of the association and Google for sharing the advertisement revenues are unilaterally and arbitrarily dictated by Google, and the members of the association have no other option but to accept the terms, as they are, with no bargaining power whatsoever. Based on this and other allegations of the association, the CCI came to the *prima facie* view that Google had violated section 4(2)(a) of the Act and directed the DG to investigate the claims.

Foreign Jurisdictions

European Union

In 2022, the EU passed the Digital Markets Act,[123] to regulate competition and ensure fairness and transparency from large digital platforms known as "gatekeepers". Gatekeepers are essentially large digital platforms providing any of the "core platform services" specified in the Act. The DMA envisages two ways to designate an undertaking as a 'Gatekeeper': either when an undertaking triggers certain thresholds specified in Article 3(1) of the DMA or they are designated as such through the exercise of the EC's residuary powers.[124] The threshold specified for designating a platform as a gatekeeper are: "(a) it has a significant impact on the internal market; (b) it provides a core platform service which is an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future."[125]

DMA imposes various prohibitions upon gatekeepers such as a prohibition on processing or cross-using data obtained through its core platform unless the notice and consent requirements under the GDPR are met[126] or using any non-publicly available data generated by or provided by business users while using the

[123] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925

[124] Article 3(8). While exercising its residuary powers in designating an undertaking as a 'Gatekeeper' the EC takes into account : (i) size, including turnover and market capitalisation, operations and position of the undertaking; (ii) number of business users using the core platform service to reach end users and the number of end users; (iii) network effects and data driven advantages; (iv) any scale and scope effects from which the undertaking benefits, including with regard to data, and, where relevant, to its activities outside the EU; (iv) business user or end user lock-in; (v) conglomerate corporate structure or vertical integration of that undertaking which may enable cross-subsidisation, combining data from different sources or leveraging of its position; or (g)other structural business or service characteristics.

[125] The above thresholds will be presumed to be satisfied if the following requirements are met: "(a) as regards paragraph 1, point (a), where it achieves an annual Union turnover equal to or above EUR 7,5 billion in each of the last three financial years, or where its average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States; (b) as regards paragraph 1, point (b), where it provides a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the Union and at least 10 000 yearly active business users established in the Union, identified and calculated in accordance with the methodology and indicators set out in the Annex; (c) as regards paragraph 1, point (c), where the thresholds in point (b) of this paragraph were met in each of the last three financial years." Vide Article 3(2).

[126] Digital Markets Act, Article 5(2).

Gatekeeper's core platform service.[127] Gatekeepers are also prohibited from tying and bundling their core platform services,[128] imposing restrictions on switching[129] or changing default pre-installed services,[130] imposing platform parity clauses,[131] engaging in self-preferencing,[132] etc.

Gatekeepers have a number of positive obligations such as enabling interoperability of third-party software applications with its operating system,[133] and providing effective interoperability free of charge to third-party hardware and software service providers for the purposes of using the gatekeeper's designated core platform service. Such effective interoperability requires gatekeepers to ensure similarity between the manners in which the third parties' and the gatekeeper's hardware and software features interact with the gatekeeper's OS or virtual assistant service.[134] Gatekeepers are also mandated to apply transparent, fair and non-discriminatory conditions to ranking, indexing, and crawling, in relation to their dealings with third-parties,[135] and required to offer choice screens on defaults and enable end users to easily uninstall default software applications in the gatekeeper's operating system, unless installing such default services is essential for the functioning of the OS or the device.[136]

Gatekeepers must provide end users with technical means, free of charge, to ensure effective portability of their data generated in their activity in relation to the core platform service.[137] Additionally, Gatekeepers must also provide business users with free of charge, continuous, real-time, and high-quality access to all data generated by business users using a core platform service.[138] The DMA further requires gatekeepers' search engines to provide third-party online search engines with anonymised access to ranking, query, click and view data generated by end users on fair, reasonable, and non-discriminatory terms.[139] In September 2023 the European Commission identified Google, Amazon and Meta as gatekeepers for Advertising Services.[140]

Australia

Australia appears to follow an integrated approach to competition and consumer protection which is evidenced through the integrated Competition and Consumer Act, 2010. In 2021 the Australian Parliament amended the Competition and Consumer Act, 2010 by passing the Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021 (**NMBC**) to address the bargaining power imbalances between digital platforms and Australian news businesses by imposing *ex-ante* standards on digital platforms carrying content by Australian news businesses. Under the NMBC

[127] Digital Markets Act, Article 6(2).
[128] Digital Markets Act, Article 5(7) and 5(8).
[129] Digital Markets Act, Article 6(6).
[130] Digital Markets Act, Article 6(4).
[131] Digital Markets Act, Article 5(3).
[132] Digital Markets Act, Article 6(5).
[133] Digital Markets Act, Article 6(4).
[134] Digital Markets Act, Article 6(7).
[135] Digital Markets Act, Article 6(5).
[136] Digital Markets Act, Article 6(3).
[137] Digital Markets Act, Article 6(9).
[138] Digital Markets Act, Article 6(10).
[139] Digital Markets Act, Article 6(11).
[140] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

corporations may be classified as 'Designated Digital Platform Corporations'[141] and one or more services in relation to a corporation may be specified as a 'Designated Digital Platform Service'[142] based on two factors: (i) there is a significant bargaining power imbalance between the corporation and its related bodies corporate, and Australian news businesses; and (ii) whether the corporation and its related bodies corporate have made a significant contribution to the sustainability of the Australian news industry through agreements relating to news content of Australian news businesses (including agreements to remunerate those businesses for their news content).[143]

The NMBC imposes data-sharing and fairness obligations on "Responsible Digital Platform Corporations"[144] insofar as their Designated Digital Platform Services are concerned.[145] Responsible Digital Platform Corporations must prepare a proposal for the Designated Digital Platform Service to recognise original covered news content during the distribution of such content, and consult registered news business corporations while developing such a proposal.[146] Responsible Digital Platform Corporations are also prohibited from differentiating among any news business corporations in respect of any digital service they operate or control.[147]

USA

On April 17, 2025, the

Concluding Remarks

When it comes to prohibiting anti-competitive agreements and abuse of dominance traditional competition law used to adopt an *ex-post* approach, i.e. the regulators intervened only after the occurrence of an anti-competitive practice. Certain aspects of the *ex-post* framework, including the time-consuming nature of enforcement proceedings, may not be appropriate for digital markets, given the unique characteristics of such markets. It is due to this drawback that regulators and stakeholders are now discussing an *ex-ante* approach to deal with competition law issues in the digital market.

---

[141] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021, Section 52E(1).
[142] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021, Section 52E(1).
[143] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021, Section 52E(3).
[144] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021, Section 52A. A Responsible Digital Platform Corporation is "a corporation that: (i) is a related body corporate of the service's designated digital platform corporation; and (ii) if the corporation is not incorporated in Australia, is managed in Australia; and (iii) either by itself or together with other corporations, operates or controls the designated digital platform service in supplying services used by Australians. If no corporation satisfies such criteria, the service's designated digital platform corporation will be the responsible digital platform corporation."
[145] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021, Sections 52R and 52S.
[146] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021, Section 52X.
[147] Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Act, 2021, Section 52ZC.

The European Union has adopted this approach in the Digital Markets Act and has even notified three entities as gatekeepers for digital advertising services. Australia uses such an approach in the digital news service sector.

As far as India is concerned, the Committee on Digital Competition Law (**CDCL**) constituted by the Ministry of Corporate Affairs observed that the current *ex-post* framework under the Competition Act, 2002 needs to be supplemented to better address concerns related to alleged anti-competitive practices of large digital enterprises. It appears to have taken inspiration from the EU regime and recommended that *ex-ante* measures be introduced to complement the current *ex-post* framework by identifying large digital enterprises with a 'significant presence' in India in selected 'core digital services' and setting predetermined rules for their conduct. However the Committee also warned that such *de novo ex-ante* framework should be implemented in a manner that does not hinder opportunities and incentives for innovation for small enterprises, and that such enterprises are not burdened with additional compliance obligations.[148] Such an approach was also suggested earlier by the Parliamentary Standing Committee on Finance in its Report on Anti Competitive Practices by Big Tech Companies.[149] Following up on its recommendation of *ex-ante* provisions for digital markets the Committee on Digital Competition Law in its report has also suggested a Draft legislation named the Digital Competition Bill, 2024 which identifies ten digital services as "core platform services" for the purposes of ex-ante intervention based on factors such as weak contestability, a higher propensity for anti-competitive practices, and the potential to impact a large number of end users and business users.[150]

[148] Report of Committee on Digital Competition Law, Ministry of Corporate Affairs, February 27, 2024, pg. 93.
[149] https://loksabhadocs.nic.in/lsscommittee/Finance/17_Finance_53.pdf
[150] Report of Committee on Digital Competition Law, Ministry of Corporate Affairs, February 27, 2024, pg. 98

CONCLUSION

With the advent of digital technology, the advertising landscape globally has undergone a transformative evolution, driven by rapid technological advancements and changing consumer behaviour. The regulatory framework in the digital advertising landscape is still evolving with regulators grappling with the technological advances in the sector and trying to ensure that an appropriate regulatory framework is put in place for the same. The primary focus of regulatory efforts is, and should be, to strike a delicate balance between fostering innovation and protecting the interests of consumers and fair competition.

One of the pivotal areas of concern is the prevalence of deceptive and manipulative advertising practices, collectively referred to as "dark patterns". These practices, which exploit cognitive biases and subvert consumer autonomy, have drawn widespread criticism from consumer advocates and policymakers alike. Across various jurisdictions, regulatory frameworks are being established to prohibit such practices, so as to ensure transparency, fairness, and respect for consumer choice in the digital advertising ecosystem. In the European Union, the Digital Services Act and the European Data Protection Board's guidelines on dark patterns have set forth comprehensive measures to combat these practices. Similarly, in India, the Guidelines for Prevention and Regulation of Dark Patterns, issued by the Central Consumer Protection Authority, have outlined specific prohibitions and requirements to safeguard consumer interests.

Since the collection and processing of vast amounts of personal data are fundamental to the business models of most players in the digital advertising landscape, data protection and privacy have emerged as critical considerations in the sector. Comprehensive legislations like the General Data Protection Regulation (GDPR) in the European Union and the Digital Personal Data Protection Act in India have established better frameworks for data governance, consent mechanisms, and individual rights which could significantly impact the digital advertising industry, necessitating changes in data handling practices, transparency, and business models. The requirements for explicit, informed consent and data minimization principles are likely to disrupt traditional approaches to data collection and targeted advertising, potentially favouring publishers and platforms with direct consumer relationships over third-party ad networks.

Competition law regulators are also closely scrutinising the digital advertising market, which is dominated by a few major players. Initiatives such as the Digital Markets Act in the European Union and the proposed Digital Competition Bill in India aim to introduce *ex-ante* regulations to prevent anti-competitive practices and promote fair competition in digital markets. These measures seek to address issues such as self-preferencing, data leveraging, and the acquisition of potential competitors by dominant platforms. Similarly jurisdictions like Australia have implemented sector-specific regulations, such as the News Media and Digital Platforms Mandatory Bargaining Code, to address bargaining power imbalances and ensure fair remuneration for news content.

While the regulatory landscape is still evolving and adapting to the dynamic nature of the advertising technology sector, it is evident that a collaborative effort among policymakers, industry stakeholders, consumer advocates, and competition authorities is crucial to ensure a transparent, ethical, and competitive digital advertising environment. Effective enforcement mechanisms and continuous adaptation to technological advancements will be key to fostering a responsible and sustainable

advertising technology ecosystem. As regulators continue to grapple with the complexities of the digital advertising landscape, they must remain vigilant and responsive to emerging challenges.