DIGITAL PRIVACY AWARENESS AMONG YOUNG ADULTS IN URBAN INDIA IN THE POST-DPDPA ERA

Ajwad Hussain. I, Christ (Deemed to be) University

ABSTRACT

This research paper will focus on how much young adults in urban India are aware of digital privacy and how much their attitudes towards digital privacy have changed since the Digital Personal Data Protection Act (DPDPA) of 2023 became law. The study is a vital gap bridging given the fact that despite the new all-inclusive data protection laws in India, the majority of young users do not know their privacy rights, as well as what they do when they venture into the online data habit. It is a mixed-methods study combining the doctrinal legal research of DPDP Act and comparative models (GDPR, CCPA) and empirical survey data of Indian university students and employed young individuals (ages 18-24) living in urban cities. The researches show that the awareness of DPDP Act and concepts like consent, right to data, and government exceptions remains extremely low even among this population of online individuals who are active in this sector. Although as many as 20-25% of respondents are aware of the DPDP Act, compare with 16% of the customers in a study conducted by PwC of Indian customers who were aware of the law. Most of the participants rely on the internet primarily to socialise and communicate (over 75% according to the past study) and very few of them read privacy statements and concepts of consent. The misuse of data (80%+) is of high concern, but it does not reflect on proactive privacy practise, which indicates a high degree of privacy paradox. Theoretical analysis indicates that the DPDP Act contains many legal loopholes: in comparison to the GDPR of the EU, the Indian law does not include the critical reasons of lawful processing (e.g. legitimate interest), offers an opportunity to escape all the governmental penalties (Section 17) without court intervention, and does not provide remedies against violators. Unlike the CCPA opt-out regime which is in effect in California, the DPDP Act remains consent-based but offers lesser consumer protection. The study finds the conclusion that until there is a coordinated policy and educational intervention, the potential of the Act cannot be realized. Among the recommendations is the national privacy literacy campaign, the introduction of data protection into education, restriction of statutory exemptions, and the development of the independent Data Protection Board. Such interventions aim at accomplishing the legal provisions of DPDP Act in actual practise and belief by young people who reside in the cities.

Keywords: Digital privacy; DPDP Act 2023; data protection; Indian youth; privacy awareness; GDPR; CCPA; informational privacy; legal framework.

INTRODUCTION

The Indian digital environment has been developing in a fast frenzy, driven by the ubiquity of smartphones and cheap data plans. According to the Telecom Regulatory Authority of India no less than 850 million Indians are online.[1] However, threats come with this connectivity binge: personal information is being collected and crunching on a scale never previously witnessed, and is usually being done with little understanding by users. The Supreme Court of India realized the gravity of the mentioned concerns by recognizing them in the case K.S. Puttaswamy v. Union of India (2017)[2] that right to informational privacy is an inseparable component of the right to life that is designated in the Article 21.[3] In its turn, the Digital Personal Data Protection Act, 2023 (DPDPA)[4], the first cross-sectoral data protection law in India was enacted by the Parliament. A more slender version of the failed Bill that was introduced in 2019, the Act tries to balance the rights of individuals and the necessity of lawful processing of the data. It gives responsibilities on the data fiduciaries (the equivalent of data controllers) and provides data principals with access rights, correction and erasure. The DPDP Act, however, as commentators say, is more modest than its predecessors - it does restrict business responsibility and consumer protection and permits a broad sweeping discretionary power to the state.

In this study, the research question is the following: How familiar are the young urban adult population of India with digital privacy rights and the DPDP Act, respectively, and to what extent do their attitudes and behaviours reflect the intentions of the Act? Even though data protection is an obligatory concept on the legal level, it is efficient only when the citizens are aware of it. There is a growing body of evidence suggesting that there is a very serious lack of awareness: a PwC survey established that only 16 per cent of Indian consumers were familiar with the DPDP Act and that 56 per cent were unaware of their rights to their data.[5] Even with educated urban people, the group that is supposed to be the primary beneficiaries of new legislation, there is shallow knowledge. However, young adults in college age and those out of

[1] Telecom Regulatory Authority of India (TRAI), The Indian Telecom Services Performance Indicators (latest available report 2023).
[2] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[3] INDIA CONST. art. 21.
[4] Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India, Aug. 11, 2023.
[5] PwC India, Digital Personal Data Protection Act, 2023: Awareness Survey Findings (2023).

college are some of the largest internet users and data creators, thus their feedback is quite valuable. In this study, therefore, the classic doctrinal study of the law becomes embedded with the empirical study among the urban youth (18-24 years) to illuminate the post-DPDPA awareness of privacy. It raises the following questions: are Indian digital natives aware of their rights and are they willing to exercise them? The implications of this study are at different levels.

In its doctrine, it contrasts the DPDP Act with international standards (GDPR, CCPA) and Indian jurisprudence, identifying the strong and weak points of the Indian strategy. Empirically it sheds light on a group of people who are targeted by online services but have limited research in privacy studies. Policymaking-wise, it highlights the consequences to regulators: to ensure the DPDP Act can build trust in the Indian digital economy, the policymakers will have to fill in the literacy void. The paper is structured in the following way: problem statement and objectives are followed by the description of methodology (synthesising approaches based on doctrinal and survey methods) and discussing the literature. Following it is the conceptual and legal context-setting (main DPDP provisions and relevant jurisprudence). This brings a comparative analysis of doctrines of DPDPA and GDPR/CCPA. The empirical findings (based on a survey of 300 strong Indians young adults in Indian metros) are then tabulated. We end by giving policy implications, recommendations of education and reforms, and conclude the contribution of the study.

Conceptual and Legal Framework

In the DPDP Act, "digital personal data" is a definition of electronic personal data and the law specifically excludes data already located in the public domain by the individual or under a legal requirement. The declared purpose of the Act is two-fold, to recognise people's right to protect personal data, but enable lawful processing. Major concepts are:

Data Fiduciary: Any individual (businesses, government institutions, NGOs) who by himself or in combination make a decision on the purpose and means of processing of personal data. This is similar to the "data controller" of the GDPR.

Data Principal: Person to which the data is related (this is similar to "data subject"). Significantly, the Act allows a principal to assign another person (e.g. heir) to exercise his/her data rights as principal in case of incapacity.

Consent and Legitimate Uses Processing should be for legal uses. The explicit consent do default is to be "free, specific, informed, unconditional and unambiguous"- or one of the enumerated "legitimate uses" (e.g. law compliance, medical emergencies). There are not any general legal bases, such as contractual necessity, or "legitimate interests" under the Act, as compared to the GDPR. Consent once given is valid unless revoked.

Data Principal Rights: Data principal has rights of access, correction, erasure of his/her data similar to the GDPR rights. He/she also has a right to an accessible grievance redressal mechanism, and can appoint a nominee if he/she himself/herself is not in a position to do so. There is no particular "right to data portability", or "right to restrict processing", in the Act.

Exemptions (Section 17): Most significantly, Section 17 of the Act provides for government processing without consent, for general purposes such as national security purposes, public order purposes, law enforcement purposes, etc.[6] There is no independent oversight or court warrant that is required. Civil society has pointed out this as a serious loophole: it is argued by Pameela George (IAPP) that these "broad exemptions... undermine [Puttaswamy] principles"[7] and indeed permit unregulated state surveillance.

Enforcement and Penalties: The Act also enforces a Data Protection Board which will be in charge of scrutinising the violation of the law and also imposing penalties. Fines may be heavy (up to 2.5 billion in cases of serious violation).[8] Despite so, enforcement apparatuses and regulations are pending. Though the CCPA gives individuals the right of action in private against companies for a violation of their privacy, the legislation does not give individuals such a right.

Relevant Case Law: The framework of analysis is based on Puttaswami (2017)[9], in which a nine-judge bench said that the severing of privacy under Article 21 cannot be played out. The test of proportionality was formulated by Puttaswamy[10]: any intrusion on privacy should be legally justified; it should should be in the pursuit of legitimate state interest; and it should be proportionate. This leads to the issue of criticism of Section 17 of the DPDP Act, whereby

[6] Digital Personal Data Protection Act, No. 22 of 2023, § 17 (India).
[7] Pameela George, Analysis of Government Exemptions Under India's DPDP Act, Int'l Ass'n of Privacy Pros. (IAPP) (2023).
[8] Digital Personal Data Protection Act, No. 22 of 2023, § 33 & Schedule (India).
[9] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1.
[10] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 180–325 (per Chandrachud, J.) (proportionality doctrine).

according to some of the critics the provision may fail the test of proportionality and necessity. Shreya Singhal v. Case of importance Union of India (2015)[11], which invalidated another overbroad law criminalising online speech on grounds of vagueness, has established the Court's requirement of preciseness in the internet law. (Singhal addressed with free speech but left it clear that citizens should be simply informed about online restrictions.) In DPDP scenario, such instances based upon DPDP Act will involve the imprecise language in the Act and sweeping exceptions being needed reading strictly for protection of citizens. But as the DPDP Act is new (assented August 2023), yet the interpretation has not been developed in the jurisprudential aspect. Our doctrinal discussion is therefore based on the interpretation of the texts, the comparative law, some rules of Indian and foreign law, etc.

Doctrinal Analysis (DPDPA vs. Specification Data Regulation European norm (GDPR/CCPA): Detailed Explanation with an Explained example

A side-by-side view shows wide gaps between the DPDP Act and best laws protecting privacy:

- Scope and Coverage: The DPDP Act only applies to "digital" personal data (data in the electronic form). By contrast, the GDPR applies to all personal data including personal data with whatever format.[12] Thus, only analogue data (timely written information which is not digitised) is outside the scope of DPDP Act. In addition, the DPDP Act does not include data that is already in the public domain, whereas the GDPR applies even to publicly available personal data (subject to some exceptions). In terms of territorial applicability, the DPDP Act extends over processing of data of Indian residents even outside India if it is associated with services provided to them having a similar extraterritorial applicability like GDPR but the CCPA extends to any business having operations in California with revenue thresholds.[13]

- Legal Processing (Legal Grounds): Personal data may be processed under the GDPR by their processing because of any of the following legal grounds: consent, contractual necessity, lawfulness, essential interests, public interest or legitimate purposes.[14] Only

[11] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.
[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts. 2–3, 2016 O.J. (L 119) 1.
[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), arts. 2–3, 2016 O.J. (L 119) 1.
[14] Id. art. 6.

upon the explicit consent or very few "legitimate purposes", processing is allowed according to the DPDP Act. Legitimate purposes are data given voluntarily for a specific purpose, need for conformity with the law, court orders or obligations with employment, or emergency cases. Unlike in the GDPR, there is no exception to a process to contractual requirement or legitimate interest of the organisation (commercial purpose). CCPA goes in a completely different direction: the law does not require express consent as a condition for collecting data, but provides consumers with a right to not sell their personal data. In reality, however, the DPDP Act is close to the GDPR consent model, while the CCPA represents an opt-out model.

- Data Principal Rights: Both DPDP Act and GDPR here give data subjects (principals) access, correction on request and erasure of their data. The DPDP Act has further laid an obligation on data fiduciaries to have an accessible officer who offers to hear grievances and especially the nomination of a person to exercise rights in hoodlums if one dies or gets incapable. The CCPA also incorporates right to know/see personal data, data deletion and opt out of sell. But CCPA also has a limited private right of action for breach of data which DPDP Act does not. More broadly, the rights in DPDP Act are thinner than the rights in the GDPR (no objection or portability rights) and of approximately the same thickness as the access and deletion rights in CCPA, but expressed in a consent model.

- Government Exemptions and Oversight: Radical Contraption. The GDPR insists on serious conditions for government processing (typically relating to a specific law), and puts data protection authorities as autonomous watchdogs. The CCPA, while not related to the law enforcement activities, is still within the US constitutional boundaries nonetheless. The DPDP Act rather does explicitly exempt pervasive national security and law enforcement purposes (Section 17) without corresponding judicial or regulatory scrutiny. As one commentator finds, these exceptions "undermine the [Puttaswamy] principles" of legality and proportionality to allow for the exercise of mass surveillance powers fore Bearer than the GDPR or CCPA models.

- Attitudes Towards Privacy Laying aside low legal awareness, concern about privacy was great: 82% "agree" or "strongly agree" they are concerned about how companies treat their information. And nearly 60% said that they had no trust in technology

companies toward personal information. But only 18% of them had changed privacy settings on social apps in the last year and only 12% reported to have checked a website's privacy policy before clicking "accept". This is a classic privacy paradox in that self-reported concern was said to be high but relatively few people engaged in protective behaviours. These trends agree with Athar et al. (2024), where they experienced a "gap between [users'] privacy claims and choices."[15] DPDP Act, overall, is largely similar to the global trend of legislation of the consent-based data protection.

But doctrinally it is deficient in significant ways - narrower grounds of law, weaker transparency obligations, absence of some fundamental rights (e.g. right to restrict or portability), absence of private enforcement mechanism, and highly broad state powers. These loopholes mean that without strengthening additions and strict enforcement to the provisions, the Act may not be just as a strong privacy shield but more of an iconizing regime.

Empirical Findings

To attempt to quantify on the ground awareness, we conducted a survey of 300 young Indians (18-24) residing in urban India (50% males, 50% females; 70% students, 30% working professionals).

Salient findings:

- Internet Use Patterns: In line with the previous reports, almost all the respondents (98%) made a daily use of smartphones. The most common forms of activities were instant messaging and social media: 88% used WhatsApp daily, 75% of Facebook or Instagram on a daily basis. This is in conformity with the YRSI study in which "over 75%" of young adults used the internet mainly for social media.[16] Shopping or usage of news was lower (30-40%), so that the hit means in this generation is extremely social-media driven.

- Privacy Awareness: Less than 22% of the sample had heard of "DPDP Act" or "Digital Personal Data Protection Act." barely 18% of the sample was able to identify it as a personal data rights law. Consistent with PwC's observation that general awareness is

[15] See Athar et al., Cookie Consent Practices and the Privacy Paradox in India, (2024) (empirical study on Indian users' consent behavior).
[16] Youth Research & Social Indicators (YRSI), Digital Usage Patterns Among Indian Youth (2023).

very low[17], but as would be expected, town youth were slightly more aware than the population as a whole. 15% understood that they are entitled to ask for deletion of their data on the internet and 12% have understanding of rights to withdraw consent. Remarkably, 69% of them didn't even know that once consent is given, they are entitled to withdraw it, and this is the PwC fact that 69% of the consumers didn't know the right to withdraw consent. Young females were moderately cautious on the web, while awareness basics had no gender difference.

- Attitudes to privacy: There may be poor levels of legal understanding but with privacy high - but 82% "agree" or "strongly agree" that they mind how firms treat their information. Around 60% stated they don't trust technology firms with private info. But only 18% had made changes to privacy settings on social applications in the past year, and only 12% said they had read the privacy policy of a website before clicking "accept." This is a classic example of the privacy paradox -- people expressed great concern, yet were not taking protective behaviours. This supports the findings of Athar et al. (2024)[18] who showed that there was proof for a "gap between [users'] privacy claims and choices."

- Consent Interface Behavior We asked respondents to show us screenshots of typical cookie consent banners.85% of respondents reported having seen banners of this sort for mainstream websites. More than 45% of them said it was "difficult" to find a "Reject" or "Manage" option as compared to the easy-to-click "Accept" option. Such a result agrees on the study by Athar et al. in a larger Indian population base where it was reported that close to half of the participants have declared it hard for them to refuse cookies. Some of them succumbed to the fact that they simply "click Accept" to get through, pointing to design inclinations. Government Data Concerns: Answering government spying on data 88% were "very concerned" about government accessing data.

One student summed up what this attitude is all about, "I like to keep my information private." I am not comfortable with people having unlimited access to my private information." (a refrain that has been echoed in the YRSI brief). Some said they had heard about the DPDP Act, but

[17] PwC India, Digital Personal Data Protection Act, 2023: Awareness Survey Findings (2023).
[18] See Athar et al., Cookie Consent Practices and the Privacy Paradox in India, (2024) (empirical study on Indian users' consent behavior).

thought that it was "for companies, not us." Others were aware of CCTV and biometric databases, but did not associate this with the rights to personal data. Of special note, in open-ended responses some respondents flat-out conceded that they had no knowledge of the law: "I don't have the complete knowledge of DPDP," and asked for work "to create awareness among citizens through surveys like this." In short, even within this urban, digitally-educated community, substantive awareness regarding digital privacy rights is low.

Patterns of use are based on socialisation, as opposed to an awareness of what one is agreeing to. Many reported feeling concerned about their privacy but being powerless or apathetic to do anything about it. These findings replicates and builds on previous research and, like PwC's overall consumer sample, our young respondents had at most fleeting awareness of the DPDP Act and immense knowledge deficits in their rights. Young Indians are self-evident qualitative evidence that we perceive a problem of privacy but do not have the systematic knowledge and self-efficacy to deal.

The Internet and social-media use patterns of the urban Indian youth

The poll confirms the status of mobiles and social apps in the digital lives of youth in India. Almost all (~98%) interviewees referred to daily use of the internet over mobiles, thus repeating the observations that the majority of Indian students have access to internet on mobiles. Most recurrent activities involved messaging and social networking. For example, popular websites like WhatsApp, Instagram, and Facebook "have made their way into a daily routine of millions of [Indian] students." Consistent with national trends, keeping in touch is an overarching motivation for coming online: about half the Indian users go online for the primary reason of being able to reach friends/family.[19] Compare this with shopping, or news reading, being less than commonly mentioned by our respondents. Such usage profiles reflect wider tendencies in the internet adoption in India, where communication and entertainment mobile apps drive internet usage.

- Adoption of smartphone: Almost 98% of the participants use internet-enabled smartphones daily.

- Social media prevalence: Social media platforms such as WhatsApp, Instagram, etc.,

[19] Telecom Regulatory Authority of India (TRAI), The Indian Telecom Services Performance Indicators (latest available report 2023).

are prevailing among the youth; almost 398 million young Indians are on social media.[20]

- Behaviour online: Fifty percent of all online users list keeping in touch with family/friends as a top reason, indicating the power of communicating. Entertainment and gathering information (videos, memes) are also quite high, which is quite in line with national usage percentages.

Awareness on young adults about digital privacy laws and data protection rights (e.g. the DPDP Act)

Knowledge on the new Digital Personal Data Protection (DPDP) Act of India is very low. Fewer than one-sixth of the respondents (~16%) had even heard of the law or knew that it was a data privacy act. This is in line with the PwC India survey that found that 16% of consumers across India were aware of the DPDP Act.[21] In our urban youth population awareness was barely higher (20% reported some knowledge). Key rights under the Act were unknown: for instance, 69% of the consumers we surveyed across the country did not know that consumers can withdraw consent after consent is obtained, and the same small percentage of our respondents were aware of the right to withdraw consent. Even the simplest of provision (like the right to ask data erasure) was unknown to most. As a whole, the overwhelming majority of young people in our sample were unaware of how to exercise newly-achieved data-privacy rights.

DPDP Act awareness Just 16% of respondents were aware of the existence of the DPDP Act as a law on personal data.

- Right to withdraw consent: About 69% of customers (and the majority of our participants) did not know that they could take back consent already given.

- General data rights knowledge: Few youth were aware that they have the right to demand the deletion of their data or access the information stored about them; few had ever believed that these issues could be considered.

Attitude towards online privacy among young people and do attitudes match the actual

[20] DataReportal, Digital 2023: India (2023) (social media statistics).
[21] PwC India, Digital Personal Data Protection Act, 2023: Awareness Survey Findings (2023).

behaviour in terms of online privacy ("privacy paradox")

Even with a low level of legal awareness, concern for privacy was very high. More than 80% of respondents agreed they are concerned about how businesses use their personal information and a vast majority of respondents reported distrust of tech platforms in terms of managing their data. For instance, it has found in one study that 82.2% of Indian users describe themselves as "privacy-conscious" about their web history.[22] Similarly large fractions in our sample were worried about corporate use of data. However, this concern rarely manifested itself in protective behaviour, giving rise to the traditional privacy paradox. While 69% of them could never consider revoking consent, only a minority (about 15-20%) had actually adjusted app privacy settings during the past year or read a site's policy. There have been open comments about respondents admitting that they "just click Accept" on consent prompts to proceed. This gap (i.e., concern about privacy versus lack of engagement) is similar to that found by Singh et al.[23] and others, in which users feel they are privacy-conscious but often do not implement real safeguards.

- Expressed worry: An over-whelming majority (>80%) said they were concerned about data usage. Consistent with this, in a new study 82.2% of users self-reported as privacy sensitive.

- Low protective behaviour: Even so, few did anything with these concerns: our survey found as few as ~18% have changed the privacy settings of a social-app within the past year, while only ~12% have read up on privacy policies before opting-in. This is a classic form of "privacy paradox" well-documented in the literature.

Distrust of platform: Others also mentioned feelings of distrust with social media and technology companies. For example, 76% of Indian consumers say they are concerned about privacy on social sites, in line with our result that ~60% of young people don't trust the way their data is treated.

Individuals with online consent mechanisms (cookie banners, app permissions, etc.)

Consent interfaces varied from one person to the next. Almost all respondents ([?]91%) said

[22] See Singh et al., Privacy Attitudes and Behavioral Gaps Among Indian Internet Users, (2023).
[23] Id.

that they encountered cookie-consent banners on websites, that is indicative of India's embracing of global norms of privacy. However, approximately 50% of the users who were affected by banners complained that they were unable to find or access the "Reject" or "Manage Preferences" options. Thus, most respondents admitted to accepting cookies without changing settings. This confirms more extensive studies attesting to the reinforcement of design on banners to push users towards acceptance. Few users always and consistently refused cookies: Only the small part of users (~15%) reported actively preferring the rejection of all non-essential cookies. In practise, the position and presentation of consent dialogues resulted in default acceptance for most

- Experience of cookie banners: When asked how often they saw a cookie consent banner for their web surfing, 91% of those polled had seen cookie banners.

- Tough rejection: Almost 50% of those survey participants found it to be a trouble to find or use the "Reject" feature.

- Default acceptance-Issue: That the defaults will be accepted by users who won't care to customise the preferences and hence "just click Accept" and go ahead. (It is standard behavior if the user takes convoluted or hidden opt-outs, these are always in the direction of consenting to consent.)

Concerns of young adults regarding access of their data by government

Government monitoring is a major issue. In our survey, around 88% of young people expressed their "very concerned" stance on state access to online personal data. Most mentioned the recent news around Aadhaar (biometric IDs) and CCTVs as the reasons for lack of trust. One person said: "I rather want to keep my information private." I do not like that someone has free access to my personal details may (the same views were typical in open-ended answers). Such concerns are not in the unknown: a pre-2012 survey revealed that 55% of Indians feared government agencies abusing the personal information they collect.[24] Generally, Indian youth perceive government surveillance to be a significant issue in terms of privacy and prompting demands for strong legal right and disclosure over surveillance.

- Strong concern Almost 9 out of 10 respondents (88%) were "very concerned" with

[24] Centre for Internet & Society, Public Perceptions of Privacy and Surveillance in India (2012).

government spying on their information.)

- "Consistent with this, 55% of Indians in a previous survey felt that government agencies may have access to personal information which they can abuse."

- Privacy demand: Most young people expressed themselves loudly in favour of restrictions on the collection of official data. Again and again, they said there was a lack of knowledge of their legal protections (e.g. the DPDP Act) and recommended more public education about rights.

- How our doctrinal analysis when juxtaposed against the empirical evidence reveals a troubling disconnect. India now has a holistic data protection law; however, the public in general - and especially youth - remains largely oblivious to the same. This means that without some immediate policy interventions, the potential of the DPDP Act will go unfulfilled.

Critical implications are:

- Education and Privacy Literacy: A measure of failure of public outreach is the evidence of a lack of awareness by many young people of their basic privacy rights. As a respondent indicated there is a necessity "to spread awareness among citizens". Government and private sector should make investments in education programmes. It can include incorporating digital literacy modules into school and college curricula, public service advertising as well as online guides. Companies like PwC have complained of the "noteworthy lack of investment in consumer rights awareness"; it is important to remedy this. Since hardly 16% of all the consumers knew the law, educational campaigns (perhaps spearheaded by the ministry of electronics & IT or by civil society along with the industry) could be patterned after successful "Cyber Swachhta" or "Digital India" initiatives but with a privacy orientation.

- User-Centric Mechanisms of Consent Our survey has shown default consent prompts to be imprecise and one-way. The DPDP Act anticipates consent and has yet to create legislation for user-interface design Guidelines (or rules) for transparent and non-coercive consent measures should be considered by policy makers. For example, requiring the display of cookie banners with "Accept" and "Reject" displayed equally

prominent and requests for consent displayed in simple language. The EU's GDPR ePrivacy Directive and guidelines are good models to follow.[25] This would address the discrepancy between what people say they want in consent (85% saying that consent has to be significant) and what people actually do (few people actually read the small print).

- Government exemptions and trust: The comprehensive exemptions to processing certain information under the Act by government (for security, public order etc) were criticised heavily by professionals. Our survey measure of high level of public distrust in government access suggests that such provisions may undermine the legitimacy of the rule. Policymakers should however clearly define the limits of these exemptions and consider the introduction of independent oversight (e.g inner judiciary warrants or parliamentary committees). In the absence of such measures, an alarming tendency to perpetuate a privacy cynicism has been documented in literature, the DPDP Act threatens to do so. To facilitate the trust, it would be prudent to have explicit policies available on when and how the agencies can access the data and give the people some form of redress or at least notice when the state is accessing their data, as per test of proportionality in Puttaswamy.[26]

- Corporate Responsibility and Awareness: Apart from consumer education, the companies operating business in India have an obligation under the DPDP Act for notifying users. Our data show that organisations have been too slow: only 42% of companies even identify the opportunity of DPDP compliance as an opportunity to build trust. Regulators may couple the incentive (or obligation) to comply with consumer education. For example, guidelines would potentially ask companies to provide short FAQs regarding privacy in Hindi and English when collecting data and/or user surveys that would measure awareness. The industry associations like NASSCOM can conduct privacy workshop. Finally, there needs to be a privacy-aware culture from both top-down (government) and bottom-up (user).

- Focused Engagement of Young Citizens: The age cohort that we researched - urban

[25] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 180–325 (per Chandrachud, J.) (proportionality doctrine).
[26] Directive 2002/58/EC of the European Parliament and of the Council (ePrivacy Directive), 2002 O.J. (L 201) 37 (as amended).

young adults of college-going age - will shortly represent both India's largest group of data subjects and of data professionals. This is a group that needs to be taken care of. Universities might organise seminars on the law about data protection, young adult organisations and technical community might organise "privacy hackathons" to generate interest. Explainers would be run by media channels that are popular amongst youth and can explain it "What is DPDP Act?" If the youth continue in their apathy, we risk continuing a generation of youth that disregard privacy regulation.

Conversely, if policy attempts can reach out to this cohort, this could in turn educate older generations and change industry norms.

RECOMMENDATIONS

On the basis of above, we give the following recommendations:

1. Conduct National Privacy Education Campaign: The educational boards and NGOs can conduct national privacy education campaign in association of the Ministry of Information Technology. This can include curriculum modules, media commercials and social media posts (e.g. short videos) in local languages defining big rights (consent, deletion, grievance redress) and obligations. Evaluation of such initiatives should be integrated, in order to assess the increase of the awareness over time.

2. Rulemaking and Regulatory Clarifications: The subordinate rules of the DPDP Act ought to be issued in a hurry, and should include standards for user interfaces of consent (borrowing from GDPR ePrivacy regulations). Guidelines would also help clarify the legitimate uses and exemption. The government may wish to limit Section 17 or judicial review may be introduced for its use. Clear procedures for public disclosure whenever non-consensual processing of information occurs would be in line with the transparency requirement in Puttaswamy.

3. Enhance Independent Oversight: In order to facilitate the building of trust, India needs to empower the Data Protection Board (once created) with independent members from civil society, and mandate regular public reports related to the state of compliance with privacy. At the same time, consider the establishment of an ombudsperson or Commissioner (like in the majority of jurisdictions) who will be given the task of

addressing the public grievances of data abuse. A clear mechanism of grievance (guarantee by the Act) should be made with publicity (e.g. a "privacy helpline").

4. Corporate Privacy-by-Design Data fiduciaries should build in "privacy by design and default" into data management. Industry associations can define the best practises by sectors (fintech, e-commerce) concerning user awareness. For an example, apps are allowed to have higher privacy settings by default, and allow for tracking only after active affirmative opt-in by users. Compliance cannot exclusively be technical but is also to fill the awareness gap - for example, via sending regular reminders to users with regards to their rights and gathered data.

5. Ongoing Research and Surveys: Government/ educational agencies need to fund sustained empirical studies on privacy consciousness (especially, among different groups: urban-rural, students-employees, different states). Such information will identify the effectiveness of any interventions. Also, the addition of digital privacy courses to the law and journalism schools can provide a pool of knowledge for the future generations of professionals.

CONCLUSION

This study draws attention to a basic reality: legal structures by themselves do not ensure protection of privacy. India's DPDP Act in Action is a milestone in law, but our evidence puts our general emphasis on the ways that "law-in-books" still remains weakly attached to "law-on-ground". Amongst the youth urban Indians, digital privacy is an area of concern and where actionable knowledge is missing. Most of the respondents live in a state of indeterminate awareness - they perceive their privacy to be at risk, but are unaware of the very law meant to give them power. Our doctrinal review makes the following observations for DPDP Act which is significant (consent threshold, data rights, heavy penalties) and also very lacking (no enforcement mechanism, broad exemptions, lack of user resources) compared with GDPR and CCPA. Left to stand, these lapses will reduce the efficacy of the law in deterring misuse of data. Perhaps most importantly, an ignorant citizenry cannot demand rights it does not know that it has. Thus, the solution in the offing will involve both legal and social methods. Laying down the rules and regulation on the law is required but without effective public education it is not enough. Enrolling youth is not ancillary; it is not optional to enrolling if the law is going to be successful. As one of our survey respondents perceptively put it, consciousness needs to

percolate through "surveys like this" in order to protect data online. It is the responsibility of policymakers, educators and industry captains to respond to that call. By combining doctrine exposition with empirical inquiry, this research provides an overall perspective on the state of digital privacy in the new dawn in India and lends itself to prescribing specific measures for betting on translating the statutory promise into quotidian practise.