CCPA'S DARK PATTERNS DECISION: WHAT IT MEANS FOR DIGITAL BUSINESSES AND SIGN UP FLOWS

Most digital businesses require users to provide personal information before accessing a product or service. Registration, onboarding and account creation have become standard parts of the user journey.

The recent order against PhysicsWallah (**"PW"**) by the Central Consumer Protection Authority (**"CCPA"**) raises an important question: can a business require users to share personal data as a condition for accessing a service that is advertised as "free"?

While the order was passed under consumer protection law and not India's data protection framework, it offers useful insight into how regulators may evaluate the relationship between data collection and the services being offered. More importantly, it signals that businesses may need to start assessing product design and data collection practices not only through a data protection lens but also from a consumer protection perspective.

LEGAL BACKGROUND

The Guidelines for Prevention and Regulation of Dark Patterns, 2023 (**"Guidelines"**) were issued under the Consumer Protection Act, 2019 to prohibit user interface designs and business practices that manipulate, mislead or impair consumer choice in a manner that constitutes a misleading advertisement or violates consumer rights. The Guidelines identify specific prohibited practices such as false urgency, basket sneaking, confirm shaming, forced action and subscription traps.

The CCPA took up a suo motu case against PW examining three categories of alleged dark pattern practices on its website and application which are prohibited under the Guidelines:

01	**BASKET SNEAKING**	PW's checkout flow displayed a pre-selected donation checkbox titled "Donate for PW Foundation," which automatically added ₹10 to the payable amount unless the user actively deselected it.
02	**CONFIRM SHAMING**	When users clicked "Know More" on the donation option, they were shown emotionally charged messaging about supporting marriages, children's education, and healthcare in underserved communities. The CCPA found this language was designed to invoke guilt and moral pressure during a commercial transaction.

03	FORCED ACTION	PW advertised a range of educational courses as “free,” but conditioned access on mandatory disclosure of a mobile number and email ID, with compulsory sign-up or log-in required before any content could be accessed. **This is the focus of this piece.**

PW’s Defence

PW’s defence on the forced action allegation was that the information collected was limited to legitimate operational, academic, security, and compliance purposes. It argued the data was necessary for progress tracking, performance assessment, learning continuity, anti-piracy, and prevention of fake or duplicate accounts. PW also drew a comparison with government educational platforms such as DIKSHA and SWAYAM, which similarly require login for course access, and submitted that applying a different standard to private edtech platforms would create an unjustified regulatory asymmetry.

CCPA’S HOLDING

As per the order, the CCPA independently accessed the free courses through multiple test accounts and found that the free educational content was identical across all test accounts, without any personalisation. On DIKSHA, the CCPA observed that while users may be required to log in for certain features, the platform does not advertise those courses as “free” in the promotional sense PW used. On SWAYAM, it noted that registration is linked to assessment tests and certification — identifiable educational outcomes that actually require user identification. In contrast, PW had not demonstrated that its collection of personal information was indispensable for the provision of the content being advertised as free.

On the basis of this examination, the CCPA held that the mandatory registration requirement was “disproportionate and not reasonably connected with the stated objective” of providing personalised educational services. Presenting courses as “free” while conditioning access on compulsory data disclosure without adequately disclosing the necessity and purpose of that disclosure had the effect of creating an incomplete and potentially misleading impression about the actual conditions attached to the service. This amounted to a misleading advertisement under Section 2(28) of the Consumer Protection Act, 2019, and fell within the prohibited category of “Forced Action” under the Guidelines.

In essence, the CCPA enforced data minimisation - a principle implicit in India’s new data protection law, the Digital Personal Data Protection Act, 2023 (“DPDPA”), which requires that personal data be limited to what is necessary for the specified purpose.

GUIDANCE FOR DPDPA

This is where the order addresses one of the questions that frequently come up in discussions around DPDPA compliance. Section 6 of the DPDPA requires that consent be “free, specific, informed, unconditional and unambiguous.” Read literally, “unconditional” would mean a data fiduciary cannot condition service access on any consent at all which would make consent-based processing commercially unworkable for any digital service. However, that cannot be what the provision intends.

In the absence of guidance on how "unconditional" is to be interpreted, the CCPA order acts as a guiding light. "Unconditional" consent should be read as prohibiting consent that is extracted as the price for something the data fiduciary could deliver without it, i.e. consent whose condition is disproportionate to the service.

On that reasoning, requiring users to provide information that is genuinely necessary to create an account, process a payment or provide a service should not be problematic. Greater scrutiny may arise where access to a service is conditioned on disclosure of personal information that serves separate analytics, profiling, advertising or other commercial objectives that are not directly connected to the service itself.

THE GDPR PARALLEL

Article 7(4) of the GDPR provides that where the performance of a service is made conditional on consent to processing that is not necessary for that service, the consent is not freely given. The question is whether the processing is genuinely required to deliver what was promised. If it is not, bundling that processing as a condition of access renders the consent invalid.

The CCPA's analysis maps precisely onto this framework. CCPA has held that the data being collected by PW was not necessary for the service being offered. The condition was therefore disproportionate, and the claim of "free" access was false.

WHY THIS MATTERS IN PRACTICE

For startups and digital businesses, the significance of the order extends beyond the edtech sector. Many businesses have traditionally viewed questions around data collection as a data protection issue. The PW order suggests that the same practices may also attract scrutiny under consumer protection laws.

Businesses should therefore review:
✓ Registration flows that collect more information than is necessary to create an account;
✓ Consent notices that bundle multiple purposes into a single acceptance mechanism;
✓ Data collection practices where the business justification is not clearly communicated to users; and
✓ Product journeys that require users to take steps that are not obviously connected to the service being provided.

If personal data is being collected as a condition of accessing a product or service, it should be possible to clearly explain why that data is needed and how it relates to the service being offered. As Indian regulators continue to address digital business practices from different statutory perspectives, the PW order illustrates how closely the various legal frameworks governing digital businesses can overlap in practice.