

Research Article

Dark Patterns on the Chain: Blockchain-Enabled Consent Manipulation and Decentralised Consent Infrastructure under India's DPDP Act, 2023

Tanishk Bhawsar*, Aman Kumar Jha and Sujal Chhajed

National Law Institute University, Bhopal, Madhya Pradesh 462044, India; amankumarjha.bscllb@nliu.ac.in (A. K. J.); sujalchhajed.bscllb@nliu.ac.in (S.C.)

* Correspondence: tanishkbhawsar.bscllb@nliu.ac.in (T. B.)

Abstract: Consent is the basis of India's data protection framework. The Digital Personal Data Protection Act, 2023 (DPDP Act) created its entire lawful processing framework based on the concept of consent that must be "free, specific, informed, unconditional and unambiguous" as per section 6(1). The law enactment time coincided with the emergence of products related to blockchain identification and consent, as solutions to the very problem that the DPDP Act intends to resolve. The effectiveness of blockchain technology for securing consent records is only partially true. It can secure consent records from being changed retrospectively, but it cannot prevent the process of consent manipulation from taking place before a person accepts an agreement. This phenomenon is known as 'dark patterns,' where users are either persuaded or tricked to consent, can even occur on an error-proof consent ledger. Current study analyses the doctrinal framework of consent established by the DPDP Act and its rules and investigates the interaction between certain dark pattern classifications and the use of smart contracts and the systems of self-sovereign identity. It explores possible technical and regulatory interventions for improving this situation, using the EU experience with consent due to GDPR and Indian legislation on the subject.

Keywords: consent; dark patterns; blockchain; smart contracts; self-sovereign identity; data protection; privacy by design; consent manipulation; GDPR

1. Introduction

The DPDP Act was passed after almost six years of writing, starting from the Justice B.N. Srikrishna Committee's 2018 report. It evolved from many retracted drafts until the final version got sanction from the President on August 11, 2023 (MeitY 2018). Current DPDP law has smooth structure with less grounds for processing, and number of rights, based on strict adherence to consent, supplemented by the undisclosed category of "legitimate uses" (DPDP Act 2023, secs. 4 and 7). The requirements for valid consent are "free, specific, informed, unconditional and unambiguous" and "provided by way of clear affirmative action" (DPDP Act 2023, sec. 6(1)). The rules of the Data Protection Board and Digital Personal Data Protection Rules of 2025 further clarify the consent managers having requirements for the notice to be provided when a request for consent is made (DPDP Rules 2025).

While India was launching its overarching legislation, another relatively independent distributed ledger technology (DLT) technology was rapidly being used in registering, timestamping, and managing consent transactions. Various technical solutions have been emphasized for consent management such as consent management solutions based on permissioned blockchains, self-sovereign identity systems based on public blockchains, and data marketplaces built on smart contracts. The latter technology will be used in some sectors (Casey and Wong 2017) since blockchain can provide a record of transactions that would be difficult to alter afterwards. This is particularly advantageous where it is the responsibility of the data fiduciary to prove efficient consent (DPDP Act 2023, sec. 6(1), read with sec. 2(k)).

Blockchain may mislead to the underlying discrepancy. Dark patterns are used during the decision-making stage prior to any transaction being finalized in the ledger (Mathur et al. 2019). A blockchain does not differentiate between whether the consent button has been pressed voluntarily or something else such as a timer and other psychological tricks made a person hit the button. Once the transaction enters the blockchain, it becomes more significant than it should be. This phenomenon is known as "manipulation laundering" as its the conversion of a procedurally compromised consent into an artefact that looks, to a regulator or a court, like the gold standard of proof.

Citation: Tanishk Bhawsar, Aman Kumar Jha and Sujal Chhajed. 2026. Dark Patterns on the Chain: Blockchain-Enabled Consent Manipulation and Decentralised Consent Infrastructure under India's DPDP Act, 2023. *Digital Social Sciences* 3(2), 45-50. <https://doi.org/10.69971/dss.3.2.2026.69>



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>.

2. Consent Architecture under the DPDP Act, 2023

2.1 The Statutory Conditions

DPDP Act permits processing of personal data only for a lawful purpose, for which consent has been given or which falls within the “legitimate uses” listed in section 7 (DPDP Act 2023, secs. 4 and 7). Section 6(1) requires that consent be free, specific, informed, unconditional, and unambiguous, and be indicated through clear affirmative action, signifying agreement to processing for the specified purpose, and be limited to such personal data as necessary for that purpose (DPDP Act 2023, sec. 6(1)). Section 6(3) requires every request for consent to be accompanied by, or preceded by, a notice given by the data fiduciary describing the personal data to be collected and the purpose of processing, in a manner the rules may specify (DPDP Act 2023, sec. 6(3)). Section 6(4) gives the data principal, the right to withdraw consent at any time, and requires the withdrawal to be as easy as the giving of consent (DPDP Act 2023, sec. 6(4)). Section 7 read with the notified rules sets out the legitimate uses’ exemption, which allows processing without consent in specified circumstances, including voluntary provision of data for a specified purpose, state functions, and employment-related purposes, among others (DPDP Act 2023, sec. 7).

Two features of this design matter for the dark pattern analysis. First, the Act places the burden of proving that consent satisfied section 6 on the data fiduciary, under section 6(1) read with section 2(k)’s definition of consent manager functions (DPDP Act 2023, secs. 6(1) and 2(k)). Second, the Act does not, on its face, mention interface design, choice architecture, or dark patterns at all. The word “manipulation” does not appear in the statute (DPDP Act 2023). The closest textual hook is the requirement that consent be “free” and given through “clear affirmative action,” language that Indian courts and the incoming Data Protection Board will have to interpret without much domestic jurisprudence to draw on, since the Act is only now approaching full implementation (DPDP Act 2023, sec. 18).

2.2 Consent Managers and the Consent Artefact

The Act creates a novel intermediary, the “Consent Manager,” registered with the Data Protection Board, through which a data principal may give, manage, review, and withdraw consent (DPDP Act 2023, secs. 2(g), 6(7)– (9)). The Digital Personal Data Protection Rules, 2025 flesh out the technical and interoperability requirements for Consent Managers, including obligations around maintaining logs of consent transactions and making those logs available to the data principal (DPDP Rules 2025, rule 4 and schedule). It is precisely this requirement, an auditable, tamper-resistant log of consent transactions, that has made blockchain infrastructure attractive to prospective Consent Manager applicants and to data fiduciaries building their own consent capture systems (Matthan 2018). The Ministry of Electronics and Information Technology’s own discussion around the Consent Manager framework, following the earlier Reserve Bank of India Account Aggregator model, has repeatedly used language about “immutable” and “portable” consent artefacts, without engaging closely with how those artefacts are generated at the point of collection (RBI 2016).

3. Dark Patterns: Taxonomy and Regulatory Recognition

3.1 What Counts as a Dark Pattern

The term “dark pattern” was coined by user-experience researcher Harry Brignull for interface elements deliberately designed to trick users into actions they would not otherwise do (Brignull 2013). The Central Consumer Protection Authority (CCPA) in India issued Guidelines for Prevention and Regulation of Dark Patterns, 2023, which identify thirteen specific patterns, including false urgency, basket sneaking, confirm-shaming, forced action, subscription traps, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick questions, SAAS billing, and rogue malware (CCPA 2023). These guidelines are issued under the Consumer Protection Act, 2019, and treat dark patterns as unfair trade practice, not specifically as a data protection wrong, but the overlap with consent capture is direct (Consumer Protection Act 2019, sec. 2(47)).

Academic taxonomies categorise dark patterns along dimensions of asymmetry, covertness, deceptiveness, information hiding, and restrictive design (Mathur et al. 2019; Gray et al. 2018). Several of these maps onto consent flows with particular force. “Interface interference,” where a genuine choice is visually de-emphasised relative to a preferred choice, appears constantly in cookie banners and consent models, where the “accept all” button is a bright, large button and the “reject” or “manage preferences” option is a small grey link (CCPA 2023, annexure, “interface interference”). “Forced action,” where a user must complete an unrelated action to access a service, appears where consent to secondary processing purposes is bundled with consent to the core service (CCPA 2023, annexure, “forced action”). “Nagging,” repeated re-prompting until the user relents, appears where consent requests reappear on every visit until the desired answer is given (CCPA 2023, annexure, “nagging”).

3.2 The Gap in the DPDP Act’s Text

Unlike the CCPA guidelines, the DPDP Act does not name dark patterns as a category of regulatory concern. Section 6(1)’s requirement of “free” consent and the notice obligations under section 6(3) (DPDP Act 2023, secs. 6(1) and 6(3)) are however close to it. The GDPR is instructive here, since Article 4(11) GDPR similarly requires consent to be “freely given, specific, informed and unambiguous,” and the European Data Protection Board’s Guidelines on consent, along with its later Guidelines on dark patterns in social media interfaces, have treated manipulative interface design as a direct violation of the freely-given requirement, not a separate wrong (GDPR 2016, art. 4(11); EDPB 2020; EDPB 2023). The Court of Justice of the European Union confirmed that pre-ticked checkboxes cannot constitute valid consent under the GDPR and the ePrivacy Directive, since the affirmative action requirement is not satisfied by a default state the user must actively undo (Planet49 2019). India’s Data Protection Board has persuasive authority to reach a similar conclusion under section 6(1), and the DPDP Rules, 2025 do not currently cross-reference the CCPA’s dark pattern guidelines (DPDP Rules 2025).

4. Blockchain Consent Infrastructure: Capabilities and Limits

4.1 What Blockchain Actually Does for Consent

A blockchain-based consent record typically works by hashing the parameters of a consent event, the identity of the data principal (often pseudonymised), the purpose, the scope of data, and the timestamp, and writing that hash to a distributed ledger, either directly or via a smart contract that also encodes the permitted uses (De Filippi and Wright 2018). Since altering a block requires altering every subsequent block and achieving consensus across the network, the record is, for practical purposes, tamper-evident after the fact (Crosby et al. 2016). This solves three real problems in consent management; the difficulty of proving what consent was given and when, the difficulty of tracking consent across multiple downstream processors once data is shared, and the difficulty of executing withdrawal consistently across a fragmented data-sharing ecosystem (Millard 2018). Self-sovereign identity models built on frameworks such as Hyperledger Indy or Ethereum-based verifiable credentials go further, giving the data principal a cryptographic wallet from which they issue and revoke credentials, theoretically returning control of the consent lifecycle to the individual rather than the platform (Preukschat and Reed 2021).

4.2 What Blockchain Does Not Do

None of this technical machinery touches the moment of choice itself. The hash that gets written to the chain is a hash of whatever the interface produced, and the interface is designed, coded, and A/B tested by the data fiduciary or a vendor working for the data fiduciary, with commercial incentives that usually favour more consent, not less (Zuboff 2019). Zuboff's account of "surveillance capitalism" describes the underlying incentive structure: platforms are rewarded for maximising the volume and scope of data they can lawfully process, and consent interfaces are one of the primary sites where that maximization happens (Zuboff 2019). A blockchain does not audit intent. It audits output. If the output is a manipulated click, the chain will faithfully and permanently record a manipulated click as though it were a free one.

This creates what current study terms "manipulation laundering", in three stages. First, the interface layer produces a consent event using one or more dark patterns, for example a confirm-shaming pattern where declining consent is framed as "No, I don't want to protect my data" rather than a neutral "Decline" (CCPA 2023, annexure, "confirm shaming"). Second, the consent management layer, whether a Consent Manager under section 6 of the Act or an internal system, captures that event and, because it is technically indistinguishable from a genuine consent event, writes it to the ledger with full metadata integrity (DPDP Rules 2025, rule 4). Third, the evidentiary layer treats the ledger entry as strong, arguably conclusive, proof of valid consent in any subsequent dispute, because tamper-evidence is conflated with substantive validity (Finck 2018). Resultingly blockchain infrastructure, designed to solve an evidentiary problem, ends up strengthening the fiduciary's hand in disputes over consent quality precisely because it produces an artefact of unusual apparent reliability.

4.3 Immutability as a Problem for the Right to Withdraw

DPDP Act Section 6(4) ensures the right of withdrawal of consent must be "as easy as" giving it (DPDP Act 2023, sec. 6(4)). Public blockchains, however, create a structural conflict between this right since data and metadata stored in an immutable ledger cannot be deleted (Finck 2018). The same issue is being debated on the incompatibility of the immutability of blockchain technology and the GDPR's right of erasure stipulated in Article 17 (GDPR 2016, art. 17; Finck 2018). In off-chain storage systems, only a hash or pointer is saved on-chain, while the actual data is stored in a mutable way outside the blockchain. This approach to data management somewhat defeats the idea of decentralisation because it puts the responsibility of ensuring compliance back on conventional systems of data retention, which is often regarded as counterproductive (EU Blockchain Observatory and Forum 2018, 15–18). Regarding consent, even a record of a flouting event remains on-chain. In cases where consent has been revoked, the fact that one has given it in the past is preserved in perpetuity, which may be taken against the person in dispute (Finck 2018, 28).

5. Case Analysis: How Specific Dark Patterns Interact with On-Chain Consent

5.1 False Urgency and Time-Boxed Smart Contracts

False urgency patterns, countdown timers, "only 2 seats left" messages, artificial scarcity claims, pressure a user into rapid, under-considered decisions (CCPA 2023, annexure, "false urgency"). Smart contracts that encode consent with an expiry or renewal window can technically reinforce this pattern rather than counteract it, because a contract designed to auto-renew consent unless actively cancelled within a window functions as an on-chain version of the subscription trap the CCPA guidelines specifically prohibit (CCPA 2023, annexure, "subscription trap"). The immutability of the contract logic means that even where a regulator later finds the renewal window unfair, unwinding the on-chain consequences, restitution of any data processed during the disputed period, cannot be achieved by simply editing a database record (Millard 2018).

5.2 Interface Interference in Consent Manager Dashboards

The DPDP framework's Consent Manager model requires a dashboard through which data principals view and manage their consents across multiple fiduciaries (DPDP Rules 2025, rule 4). Because Consent Managers are themselves commercial entities, typically earning revenue through fees charged to data fiduciaries or through data-adjacent services, there is a risk that the dashboard itself becomes a site of interface interference, for example by defaulting to an aggregated "accept all new requests" toggle, or by visually foregrounding fiduciaries who pay for placement (Matthan 2018). A blockchain-based Consent Manager does not eliminate this risk. It merely ensures that whatever choices are made through the interference-laden dashboard are recorded with high fidelity (Mathur et al. 2019).

5.3 Forced Action and Bundled On-Chain Permissions

Where consent to data processing is technically bundled with consent to other on-chain actions, such as wallet connection, token-based loyalty programmes, or NFT-gated access, forced action patterns become harder to unwind because the underlying smart contract may condition access to a service on a single, all-or-nothing transaction (De Filippi and Wright 2018). Section 6(1) of the DPDP Act requires consent to be limited to necessary data and, implicitly, unbundled from unrelated conditions, echoing the GDPR's Article 7(4) unbundling principle as interpreted in Planet49 and in subsequent EDPB guidance (GDPR 2016, art. 7(4); Planet49 2019). Smart contracts that are not carefully designed to separate the data-processing permission from other on-chain

permissions risk building forced action directly into the protocol layer, which is considerably harder to remediate than an interface layer violation, since it may require a contract migration rather than a UI change (Millard 2018).

6. Regulatory Gaps and the Case for Decentralised Consent Infrastructure Done Right

6.1 The Missing Cross-Reference

An immediate regulatory gap is the absence of any cross-reference between the DPDP Rules, 2025 and the CCPA's Dark Pattern Guidelines, 2023 (CCPA 2023). The two instruments currently operate as parallel regimes. One governs the substantive validity of consent under data protection law, the other governs unfair trade practices under consumer protection law, and a dark pattern that vitiates consent under section 6 of the DPDP Act may or may not also trigger CCPA action, depending on characterisation (Consumer Protection Act 2019, sec. 2(47)). A data principal harmed by a manipulated consent flow that has since been immutably recorded on a blockchain currently has to choose between two enforcement tracks that were not designed to talk to each other, before the Data Protection Board, which is still being operationalised, or before consumer protection authorities (DPDP Act 2023, sec. 18).

6.2 Design Principles for Genuinely Decentralised Consent

Any formal consent model (for a Consent Manager and a relevant curation database) be certified against CCPA's taxonomy of dark patterns before being considered compliant (CCPA 2023). Additionally, the off-chain mutable archiving of the originating consent event, with on-chain only cryptographic commitment, must be made obligatory so that withdrawal or a ruling on invalidity can be reflected in the document that the data principal will be using instead of having an immutable record that looks correct forever (EU Blockchain Observatory and Forum 2018, 16). Also, the self-sovereignty of identity models, with the data subject as custodian of their own credentials, brings it closer to the autonomy objectives than any fiduciary-controlled or platform-controlled ledger. The standard established by the Data Protection Board for the Communication Managers should be supportive of those solutions in which the data subject, rather than the fiduciary, is the one who holds the key for signing consent transactions (Preukschat and Reed 2021). If blockchain-based consent infrastructure is to deliver on its promise rather than simply harden manipulation into permanent form, several design principles follow from the analysis above. First, immutability should attach only to the fact and metadata of a consent transaction, not to a legal presumption of its validity, meaning regulations should expressly state that an on-chain consent record is evidence of what was recorded, not proof of what section 6 requires (Finck 2018).

6.3 Comparative Lessons

European Union policy serves as an incomplete template. The Digital Services Act, Article 25's ban on manipulation in user interface design, when viewed through the lens of GDPR's consent requirements, is exactly the sort of two-tier regulation unavailable in the context of India, with the DPDP Act and CCPA guidelines (DSA 2022, art. 25). The UK's Information Commissioner's Office has likewise established guidance that "nudging" strategies in cookies consent fall under the category of valid consent infringement rather than a separate offense, thereby reinforcing the interpretation of manipulation and invalidity as one and the same legal issue (ICO 2023). Once India's Data Protection Board is fully constituted, it should adopt a similar approach to section 6 where it treats any of the thirteen recognised dark patterns under the CCPA as *prima facie* evidence that consent was not "free" as required under the Act (DPDP Act 2023, sec. 6(1)).

7. Constitutional and Pre-DPDP Foundations

This is not an entirely new development. The ruling in *Justice K S Puttaswamy v Union of India* states that the right to privacy includes informational privacy as well as an individual's right to control their information (Puttaswamy 2017). Particularly, the emphasis on autonomy and self-determination, which forms privacy by saying that privacy is comprised of autonomy and self-determination, makes the consent requirements of the DPDP Act constitutional in a way that understanding section 6 simply contractually would lose (Puttaswamy 2017). Prior to the enactment of the DPDP Act, the standard of consent as per the operative principle in India, was operationally stated under Rule 5 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which did require obtaining consent in written terms in the case of using sensitive personal data, meaning that the original standard previously applicable was far less compliant with the DPDP Act (IT Rules 2011, rule 5). Considering the DPDP Act's consent principle in line with the concept of autonomy as recognised in Puttaswamy, strengthens the case we make in this article namely that manipulated consent is not just a matter of data protection law. The tamper-proof character of a piece of evidence cannot take the place of the right to autonomy (Puttaswamy 2017).

8. The EU AI Act's Provisions on Manipulative Systems

A further comparative resource, is Regulation (EU) 2024/1689 (the AI Act), which prohibits the placing on the market of AI systems that deploy subliminal, manipulative, or deceptive techniques with the objective or effect of materially distorting a person's behaviour in a manner that causes or is reasonably likely to cause significant harm (AI Act 2024, art. 5(1)(a)). Article 5(1)(a) of the AI Act does not target consent interfaces specifically, but its language of "materially distorting behaviour" through techniques the person is not necessarily aware of overlaps substantially with the dark pattern taxonomy discussed in section 3 above, and gives a second, AI-specific hook for regulating consent flows that use algorithmically optimised, personalised manipulation, for example dynamically adjusted urgency messaging generated by a recommender system rather than a static countdown timer (AI Act 2024, art. 5(1)(a)). Where a blockchain-based consent platform incorporates an AI component to personalise the consent request itself, tailoring wording, timing, or visual emphasis to the individual user's predicted susceptibility, the AI Act's prohibition would apply independently of, and in addition to, any DPDP Act analysis, since the AI Act reaches the manipulative system regardless of the sector in which it is deployed (AI Act 2024, art. 5, read with recital 29). India has no direct equivalent of this provision, and the absence is worth flagging as a further legislative gap alongside the CCPA cross-reference problem identified in section 6.1.

9. Conclusion

Blockchain technology is genuinely useful for parts of the consent problem that the DPDP Act creates, particularly the burden of proof on data fiduciaries and the practical difficulty of tracking consent across a fragmented ecosystem of processors. It is not useful, and may be actively counterproductive, for the part of the problem that matters most to the individual: whether the choice they made was genuinely their own. The risk current study has traced is not that blockchain consent infrastructure will fail to work as advertised, but that it will work exactly as advertised, producing permanent, verifiable, tamper-proof records of choices that were never free in the first place. Closing this gap requires India's data protection framework to stop treating consent as a single event to be recorded and start treating it as a process whose quality has to be assessed independently of how well it is recorded. The DPDP Act already facilitates this interpretation because it stipulates the necessity of free, informed, and unambiguous consent manifested through clear affirmative action. What this interpretation lacks, however, is a regulatory connection between such articulation and the already established taxonomy of dark patterns of the CCPA, as well as a set of technical requirements guaranteeing that the process of decentralisation is in service of the autonomy of data subjects and not merely of the convenience of fiduciaries.

References

- AI Act. 2024. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). *Official Journal of the European Union* L, 2024/1689, July 12, 2024.
- Brignull, Harry. 2013. Dark Patterns: Inside the Interfaces Designed to Trick You. *The Verge*, August 29, 2013.
- Casey, Michael J., and Pindar Wong. 2017. Global Supply Chains Are About to Get Better, Thanks to Blockchain. *Harvard Business Review*, March 13, 2017. <https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain>.
- CCPA (Central Consumer Protection Authority). 2023. *Guidelines for Prevention and Regulation of Dark Patterns, 2023*. Gazette of India, November 30, 2023. New Delhi: Department of Consumer Affairs, Government of India.
- Consumer Protection Act. 2019. *The Consumer Protection Act, 2019*. Act No. 35 of 2019. New Delhi: Government of India.
- Crosby, Michael, Pradan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. 2016. Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review*, no. 2 (June): 6–19.
- De Filippi, Primavera, and Aaron Wright. 2018. *Blockchain and the Law: The Rule of Code*. Cambridge, MA: Harvard University Press. <https://doi.org/10.4159/9780674985933>
- DPDP Act. 2023. *The Digital Personal Data Protection Act, 2023*. Act No. 22 of 2023. New Delhi: Government of India.
- DPDP Rules. 2025. *The Digital Personal Data Protection Rules, 2025*. New Delhi: Ministry of Electronics and Information Technology, Government of India.
- DSA. 2022. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union* L 277, October 27, 2022, 1–102.
- EDPB (European Data Protection Board). 2020. *Guidelines 05/2020 on Consent under Regulation 2016/679*. Version 1.1, adopted May 4, 2020. Brussels: EDPB.
- EDPB (European Data Protection Board). 2023. *Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them*. Version 2.0, adopted February 14, 2023. Brussels: EDPB.
- EU Blockchain Observatory and Forum. 2018. *Blockchain and the GDPR*. Thematic report, October 16, 2018. Brussels: European Commission.
- Finck, Michèle. 2018. Blockchains and Data Protection in the European Union. *European Data Protection Law Review* 4 (1): 17–35. <https://doi.org/10.21552/edpl/2018/1/6>
- GDPR. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). *Official Journal of the European Union* L 119, May 4, 2016, 1–88.
- Gray, Colin M., Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, paper 534, 1–14. New York: ACM. <https://doi.org/10.1145/3173574.3174108>
- ICO (Information Commissioner's Office). 2023. *Guidance on the Use of Cookies and Similar Technologies*. Wilmslow, UK: ICO.
- IT Rules. 2011. *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. G.S.R. 313(E). New Delhi: Government of India.
- Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): article 81, 1–32. <https://doi.org/10.1145/3359183>
- Matthan, Rahul. 2018. The Third Way: Privacy Should Not Be a Trade-Off with Innovation. Discussion document. Bengaluru: Takshashila Institution.
- MeitY (Ministry of Electronics and Information Technology). 2018. *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. New Delhi: Government of India.
- Millard, Christopher. 2018. Blockchain and Law: Incompatible Codes? *Computer Law & Security Review* 34 (4): 843–46. <https://doi.org/10.1016/j.clsr.2018.06.006>

- Planet49*. 2019. Case C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH*. ECLI:EU:C:2019:801. Court of Justice of the European Union (Grand Chamber), October 1, 2019.
- Preukschat, Alex, and Drummond Reed. 2021. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Shelter Island, NY: Manning.
- Puttaswamy. 2017. *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. Supreme Court of India, August 24, 2017.
- RBI (Reserve Bank of India). 2016. *Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016*. As amended. Mumbai: RBI.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.