# SOVEREIGNS OF THE DATA REALM: JURISDICTIONAL OVERLAPS AND FORUM SHOPPING BETWEEN THE COMPETITION COMMISSION OF INDIA AND THE DATA PROTECTION BOARD OF INDIA

Tejas Shukla, Amity University Madhya Pradesh

**ABSTRACT**

India spent the better part of a decade arguing about whether it needed a data protection law, and almost no time at all asking what would happen to the regulators it already had once that law arrived. The Digital Personal Data Protection Act of 2023 has now created a Data Protection Board, a specialised adjudicator for the misuse of personal data. But personal data was, by then, already being policed from another direction. The Competition Commission of India had spent the preceding years treating the way dominant digital platforms collect and exploit data as a question of market power, and in its order against Meta it fined the company for precisely that. Two regulators now look at the same conduct of the same firms and see two different wrongs. This paper asks what happens when they look at the same conduct and reach for the same firm at the same time. It argues that the overlap is real, that the statutes do little to resolve it, and that the most likely consequence is not open conflict between the two bodies but something quieter and harder to police: forum shopping, in which complainants and defendants alike steer the same grievance towards whichever regulator promises the better outcome. The trouble is not that India has built two regulators where it needed one. It is that it has built two and given them no rule for who goes first.

**Keywords:** data protection; competition law; Data Protection Board; Competition Commission of India; jurisdictional overlap; forum shopping; DPDP Act

## Introduction

There is a particular kind of regulatory mess that no one designs on purpose and everyone sees coming. It happens when two authorities, each created carefully and for good reasons, are pointed at the same conduct without anyone deciding which of them is meant to act first. India has just walked into one. The conduct in question is the way the largest digital companies gather, combine and trade the personal data of their users. The two authorities are the Competition Commission of India, which polices the abuse of market power, and the newly minted Data Protection Board of India, which polices the misuse of personal data. They were built in different decades for different purposes, and they now share a frontier neither was designed to share.

The discomfort is not that one of them is wrong to be interested. Both make a valid point. It is as much a competition problem as it is a privacy problem when a dominant platform essentially presents its users with a take-it-or-leave-it, accept sweeping data-sharing terms, or lose the platform - the exact phenomenon that occurred when WhatsApp rolled out its new policy in 2021. The Competition Commission viewed it as an abuse of dominance; had a data protection regulator then existed, it would have viewed it as compelled consent. The very same conduct has two legal interpretations. The central question of this paper is how should a legal system respond when a single action simultaneously triggers two parallel legal frameworks administered by two separate regulators, either of whom has the power to initiate action independently.

The argument made herein, briefly stated at the outset so the reader is aware of the destination, is that the overlap between the Competition Commission and the Data Protection Board is not a theoretical issue that carefully crafted wording can prevent.[1] It is a function of the subject matter itself, as data has both the characteristics of a protected individual interest and a market power resource. The Digital Personal Data Protection Act, 2023, largely fails to ameliorate the overlap; indeed, its non-obstante and civil-court-ousting clauses tend to exacerbate it. The Competition Act, 2002, remains silent on the problem, and the only guidance available from Indian courts is in cases dealing with a related overlap between the Commission and sectoral regulators such as the telecom authority. I will argue that this means that the two bodies are

[1] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 5, which obliges a data fiduciary to obtain the consent of the data principal before processing personal data.

unlikely to clash directly. Instead, the lack of a rule as to which one should proceed first gives a strategic advantage to the parties involved: a complainant will prefer to bring the matter before the body offering the stronger penalties or a more favorable legal standard, and the defendant will contest jurisdiction (as Meta has done), arguing that the matter belongs elsewhere. This is forum-shopping, and a system that promotes it even implicitly is poorly designed, even if the regulators themselves act conscientiously.

The discussion continues in six parts. Part 2 outlines the two regulatory regimes and their points of contact. Part 3 explains why data naturally falls within the purview of both regulators simultaneously, rather than exclusively in one. Part 4 discusses the WhatsApp litigation, which is the only instance to date where the overlap has been tested in practice, and interprets the reasoning of the Competition Commission and the appellate tribunal in relation to the question of jurisdiction. Part 5 addresses the forum-shopping issue more directly and proposes what, if any, doctrine can govern the sequencing of the two regulatory bodies. Part 6 examines approaches taken by other systems, as well as Indian courts, for managing regulatory overlaps. Part 7 synthesizes the findings.

One word on method and scope. This is a doctrinal essay drawing from both statutes, the Competition Commission's order against Meta, the ensuing appellate decision, and the Supreme Court's jurisprudence on overlapping regulatory jurisdiction. As no decision has yet been rendered by the Data Protection Board, and the rules under the Data Protection Act are still under development, a significant portion of this essay necessarily involves an attempt to infer future actions and to anticipate an upcoming conflict. I have made efforts to clearly differentiate where the arguments are grounded on prediction versus established authority.

**The Two Regimes and Where They Meet**

To see the overlap one has to first see the two regimes as their drafters saw them, which is to say as entirely separate things that happen to govern overlapping facts.

The older of the two is competition law. The Competition Act, 2002, gives the Competition Commission a sweeping and deliberately sector-agnostic mandate to prevent practices that have an appreciable adverse effect on competition, to curb the abuse of a dominant position, and to regulate combinations. The provision that matters here is the prohibition on abuse of

dominance.[2]

A dominant enterprise may not impose unfair conditions, may not limit the market to the prejudice of consumers, and may not use its strength in one market to protect or extend its position in another. None of this language mentions data. It did not need to. The Commission's jurisdiction follows market power wherever it goes, and the Supreme Court has confirmed that the Commission is not confined to any sector but operates across all of them.[3]

The newer regime is the Digital Personal Data Protection Act, 2023. Its centre of gravity is consent: a data fiduciary may process personal data only for a lawful purpose and, in the ordinary case, only with the consent of the data principal, and that consent must be free, specific, informed and capable of being withdrawn. Enforcement is entrusted to the Data Protection Board of India, a body designed not as a policymaker but as an adjudicator. The Board inquires into breaches, hears complaints, and imposes penalties; for the purposes of an inquiry it is clothed with the powers of a civil court.[4] The penalties it may levy are large, reaching as high as two hundred and fifty crore rupees for the gravest failures to protect data.[5]

Two features of the data protection statute do most of the work in the argument that follows, because they are the provisions that would govern any clash. The first is the clause declaring that the Act is in addition to and not in derogation of other laws, while also providing that where its provisions conflict with another law, the Act prevails to the extent of the conflict. The second is the clause barring civil courts from entertaining any matter the Board is empowered to decide.[6] The first of these is the kind of provision that promises coexistence with one breath and primacy with the next; it tells us the Act sits alongside the Competition Act until the two disagree, and then it tells us the Act wins, without telling us how to know when they disagree. The second was plainly written to stop disputes wandering into ordinary civil courts. Whether it was meant to fence out a fellow statutory regulator such as the Competition Commission is a question its drafters do not seem to have asked, and it is exactly the question a determined

[2] Competition Act, 2002 (Act 12 of 2003), s. 4, which prohibits the abuse of a dominant position by an enterprise.
[3] Competition Commission of India v. Bharti Airtel Ltd., (2019) 2 SCC 521.
[4] DPDP Act (n 1), s. 27, which sets out the functions of the Data Protection Board, and s. 28, which confers on it the powers of a civil court for the purposes of an inquiry.
[5] DPDP Act (n 1), s. 33, empowering the Board to impose monetary penalties up to the limits set out in the Schedule, the highest being two hundred and fifty crore rupees.
[6] DPDP Act (n 1), s. 38, providing that the Act is in addition to and not in derogation of other laws, and that its provisions prevail to the extent of any conflict; and s. 39, which bars the jurisdiction of civil courts in matters entrusted to the Board.

litigant will ask for them.

The point of laying the two regimes side by side is to notice how little they say about each other. The Competition Act predates the data statute by two decades and could not have anticipated it. The data statute mentions the Competition Act nowhere. Each is internally complete and externally silent. That silence is the soil in which the overlap grows.

**Why Data Falls into Both Fields at Once**

It would be tempting to treat the overlap as a drafting accident that a clarifying amendment could cure. It is not. The overlap exists because of what data is, and no amount of tidy drafting changes the nature of the thing being regulated.

Personal data has, for a single individual, the character of a right. It is information about a person, and the law of data protection exists to give that person some control over how it is gathered and used. But that very data, collected at scale from millions of users, ceases to function as a bundle of individual rights and comes to function as an asset. It becomes the source material for hyper-targeted advertising, the energy source for recommender engines, and the moat that protects a dominant firm's dominance. A company with most of a nation's users' data has a visibility into the behavior of a rivals' customers that the rivals themselves do not have; it can lock in customers within a network so powerful that it is difficult for them to leave; it can use its knowledge gained from one market to seize another. At that scale the issue shifts from whose privacy has been violated to: does the market still function?

This is why the two regulators aren't really doing the same work even when they examine the same conduct. The Data Protection Board, when examining WhatsApp's policy, would look at whether the user's agreement to share their data was freely given or was coerced as a condition for their continued use of WhatsApp. When examining the same policy, the Competition Commission would ask whether the dominant firm used its power to extract terms that a competitive market would not allow, and whether the data harvested entrenches that market power. The first is an issue of the individual and her autonomy; the second, of the market and its structure. The answers to both questions can be found within the exact same line of the exact same privacy policy.

Once that is clear, the phantom solution of instructing each regulator to stay within its lane

dissolves because the conduct is not divisible into separate lanes. The privacy lane and the competition lane both cross at the same intersection. Coerced consent is the abuse; the condition imposed in violation of the privacy of the user is the unfair condition. The Commission, instructed to ignore the data dimension of the situation, is instructed to ignore the mechanism by which the abuse is accomplished. The Board, told to disregard the market dimension, is asked to feign that the coercion of a dominant firm is somehow no different from the coercion of a small competitor.

Neither pretense will work.

**The WhatsApp Litigation: The Overlap's First Real Test**

The argument has so far been abstract, but it has had one concrete rehearsal, and it is worth following closely because it shows how the overlap behaves under pressure. In 2021 WhatsApp updated its terms of service and privacy policy in a way that required users, as a practical condition of continuing to use the application, to accept the sharing of certain data with other Meta companies. The Competition Commission took up the matter on its own motion and, after a long investigation punctuated by jurisdictional challenges that travelled as far as the Supreme Court, held in November 2024 that Meta and WhatsApp had abused their dominant position. It found that a firm dominant in the market for smartphone messaging applications had used coercive datasharing terms to fortify Meta's position in online display advertising, and it imposed a penalty of roughly two hundred and thirteen crore rupees together with directions about how the data could be used.[7]

The interesting part, for present purposes, is not the penalty but the defence. Meta and WhatsApp argued that the Commission had no business deciding the matter at all. The entire dispute, they said, was about privacy and consent. Privacy and consent were the domain of data protection law, governed by the data protection statute and the older rules on sensitive personal information, and shortly to be administered by a dedicated Board. A competition regulator had wandered into a field reserved for another. The argument was, in effect, that the conduct had only one legal face, the one the defendant preferred, and that the Commission had mistaken it

[7] In re: Updated Terms of Service and Privacy Policy for WhatsApp Users, Suo Motu Case No. 01 of 2021, order of the Competition Commission of India dated 18 November 2024, imposing a penalty of about Rs. 213.14 crore on Meta and WhatsApp.

for another.

The tribunal dismissed that argument in November 2025 and the reasoning adopted by it is important. It argued that competition and data protection law should be considered parallel to and not alternative to each other. While data protection law regulates an individual's personal data and ensures free consent is obtained, competition law focuses on whether a dominant firm employs data (personal or not) to manipulate the market, block competitors, or exploit customers. A mere overlap in subject matter, the tribunal said, does not strip the Commission of its jurisdiction. It upheld the finding of abuse and the penalty, while trimming one of the remedial directions on the ground that it was unnecessary once users were genuinely free to opt in or out.[8]

Two things follow from this episode, and they pull in opposite directions. The first is reassuring: a court has now said, in terms, that the existence of a privacy dimension does not oust the competition regulator, and that the two regimes can coexist. The second is less reassuring, and it is the one this paper presses. The reassurance was delivered in a world where the Data Protection Board did not yet exist. The Commission could proceed precisely because there was no rival regulator actually seized of the matter; the field of data protection enforcement was, in practice, empty. The tribunal's confident talk of complementary frameworks was never tested against an actual, simultaneous data protection proceeding, because there could not be one. The real test is still to come, and it will come the first time the same conduct is before both the Board and the Commission at once.

**The Real Problem: Forum Shopping in the Absence of a Sequencing Rule**

This is the problem that the paper tries to resolve. When two regulators have the power to take action against the same behavior, but no rule specifies the order in which the actions must occur, or that either one pre-empts the other, then the decision as to where the proceedings take place is removed from the regulators and placed squarely within the hands of the parties. The decision isn't neutral, since the two forums are far from identical, and a smart defendant will choose whichever one is in its best interest.

And the asymmetries are profound. The two penalties are different in both their size and in the

[8] WhatsApp LLC v. Competition Commission of India, Competition Appeal Nos. 1 & 2 of 2025, National Company Law Appellate Tribunal, judgment dated 4 November 2025.

legal reasoning behind them. The data law has a maximum penalty of two hundred and fifty crore rupees based upon the harm caused by a data breach; the Competition Act uses an entirely different model calculating penalty based on turnover and aimed at deterring anticompetitive behavior. The standards of liability are different. The Board asks whether a valid consent to the data processing was obtained, which depends on the details of that particular transaction. The Commission asks whether a company has acquired or abused dominant position in a relevant market, which involves proving a much more complex concept of dominance, market definition and effect. The two procedures, the respective paths to appeal and even the very nature of the problem each regulator is trying to redress are starkly different. The complainant who wants the highest possible penalty and whose consent claim will be more easily satisfied than a proving dominance case would go to the Board. The complainant who can't prove that the data privacy rules were violated but can show that the conduct harmed the market would go to the Commission. And the defendant, as was Meta, would claim that in all circumstances, the chosen forum is inappropriate and the case belongs to the other.

This is forum shopping in the traditional sense and that presents a real problem irrespective of how well-intentioned each of the regulators are. It makes the outcome depend on the strategic choices of litigants rather than on the nature of the wrong. It permits inconsistent findings, in which one regulator holds the conduct lawful and the other unlawful, leaving the firm and the public unsure which to believe. It risks double jeopardy, where a firm penalised by one body is pursued again by the other for the same underlying act. And it wastes the scarce capacity of two expert bodies on the same facts. None of these consequences requires either regulator to overreach. They follow simply from the absence of a rule about who goes first.

Does any such rule exist? The nearest thing in Indian law is the doctrine the Supreme Court developed for a different overlap, that between the Commission and sectoral regulators. In the telecom case the Court held that where a specialised regulator occupies the field, that regulator must first determine the jurisdictional facts that lie within its expertise; only once it has done so may the Competition Commission take up the distinctively competition-law question of whether those facts disclose an abuse.[9] The Court called this comity, a mutual respect under which the expert body goes first on matters within its expertise and the market regulator follows

[9] Bharti Airtel (n 3). The Court held that the CCI is a market regulator whose jurisdiction is not ousted in any sector, but that where a specialised statute occupies the field, the sectoral regulator must determine the jurisdictional facts before the CCI proceeds.

on matters within its. It is an attractive model, and it has the great merit of already existing.

But it transplants awkwardly to the present problem, and the awkwardness is worth being honest about. The telecom doctrine rested on the idea that the sectoral regulator possessed technical expertise the Commission lacked, so that letting it go first improved the quality of the eventual competition analysis. The relationship between the Data Protection Board and the Commission is not quite like that. The Board's expertise, in consent and data handling, is not a mere technical input into a later competition finding; it is a complete adjudication of a complete wrong, the privacy wrong, that exists independently of any market effect. Telling the Board to go first so that the Commission may then build on its findings misdescribes what the Board is doing, because the Board is not preparing the ground for the Commission. It is deciding its own case. The comity model assumes the two inquiries are sequential parts of one analysis. Here they are two separate analyses of one set of facts, and sequence does not naturally arise from the subject matter.

Nor does the data statute supply the missing rule, though at first glance it seems to try. Its clause declaring that the Act prevails over conflicting laws might be read to give the Board priority. But that clause speaks to conflict between provisions, not to the allocation of overlapping jurisdiction, and there is no conflict in the relevant sense between a law that protects consent and a law that polices dominance; a single act can breach both without the two laws contradicting each other. The clause ousting civil courts is similarly beside the point, because the Competition Commission is not a civil court but a statutory regulator with its own mandate, and the appellate tribunal has already held that a privacy dimension does not oust the Commission.[10] The statute, read carefully, neither subordinates the Commission to the Board nor the Board to the Commission. It leaves them level, and level is precisely the condition in which forum shopping thrives.[11]

The honest conclusion is that India has, at present, no rule for who goes first, no rule against being pursued twice, and no mechanism requiring the two regulators even to consult one another before acting. The appellate tribunal's language of complementary frameworks is a description of how the two regimes relate in the abstract. It is not a sequencing rule, and it will

[10]

[11] **Digital Personal Data Protection Act 2023, ss 39–40.** Section 39 gives the Act overriding effect over inconsistent laws, while s 40 excludes the jurisdiction of civil courts; neither provision establishes a hierarchy between the Data Protection Board and the Competition Commission of India.

not tell a future Board whether to stay its hand while the Commission proceeds, or tell the Commission whether a prior penalty by the Board bars its own.

**Models for Managing the Overlap**

If the statutes themselves don't do the job, the question is what could, and the obvious places to look are both to external systems and to India's own toolkit. No model is perfect, and a candid study has to be honest about the limitations.

One option would be to adopt the model of statutory primacy: an amendment to one of the two statutes to say that when both are applicable, one regulator proceeds either first or exclusively. This is both simple and crude. Subordinating all else to the Board would prevent the protection of genuine market harms if, even by chance, it also touched data, which it does in the digital economy. Subordinating data protection to market analysis would undo the data statute's premise: the public policy rationale that we don't need to be proven wrong by evidence of actual market effects to be protected against privacy risks, just that privacy is intrinsically valuable. One regulator's primacy, by definition, compromises one aspect of what the two-pronged regime was designed to serve. That is too costly.

A second option would be to take the comity model from the sector-specific regulator cases, in which the Board investigates facts pertaining to data protection, and then the Commission analyzes their significance in terms of competitive policy. For reasons already articulated in Part 5 this model works only in approximation, since the Board's fact finding is not simply preliminary to the Commission's. Still, a slightly different version of comity is workable: not that one body's findings bind the other, but that whichever regulator is approached second should ordinarily defer to the factual findings of the first on matters within that first body's expertise, while remaining free to draw its own legal conclusions. This reduces inconsistent fact-finding without pretending the two inquiries are one.

The third model is one of institutional cooperation: a Memorandum of Understanding between the two agencies-similar to what has been done by regulators in other areas-under which both will consult, will share information, and will agree how they will handle cases in the overlapping area. It has the benefit of flexibility, and the drawback of being not enforceable by the parties themselves; it disciplines the regulators but gives the litigant no recourse against the regulator who flouts the agreement. It is a helpful ancillary mechanism but is no substitute for

a rule.

The fourth model deals with the double-jeopardy strand: it appropriates a well-known rule from other areas that one should not be twice punished for one act, such that any penalty handed out by the one regulator will have to be taken into account by way of set-off or mitigation in the penalty handed out by the other. The other regulator can still punish the firm for the act; the effect is simply to prevent the firm's punishment being a combination of two unrelated penalties, and gives the defendant an argument other than a claim that the second forum has no jurisdiction at all.

It is worth adding that the appellate structure aggravates rather than eases the problem. Appeals from the Competition Commission lie to the National Company Law Appellate Tribunal, while appeals from the Data Protection Board lie to the Telecom Disputes Settlement and Appellate Tribunal.[12] Two regulators feed two different appellate tribunals, so that even at the appellate stage there is no single body positioned to reconcile their conclusions short of the High Courts or the Supreme Court. A coherent solution would do well to provide a common point at which the two strands can be drawn together, rather than leaving reconciliation to the accident of which constitutional court is approached.

The least satisfying but most likely outcome is that none of this is legislated, and the courts are left to improvise, extending the comity reasoning of the sectoral cases case by case as disputes arise.[13] That is how the overlap between the Commission and the sectoral regulators was managed, and it produced workable rules eventually, but only after years of contradictory High Court decisions and considerable cost to the parties who happened to be the test cases. There is no reason to expect the data overlap to be resolved more quickly or more cheaply if it is left to the same process, and good reason, given how fast the digital economy moves, to wish it resolved before rather than after the litigation teaches the lesson.

## Conclusion

Where does this leave the relationship between the two sovereigns of the data realm? So on the small question of whether either has the right to bring an action against a data-related action,

[12] DPDP Act (n 1), s. 29, providing that an appeal from an order of the Board lies to the Telecom Disputes Settlement and Appellate Tribunal.
[13] Competition Commission of India v. Bharti Airtel Ltd. (n 3); see also Coal India Ltd. v. Competition Commission of India, (2023) 10 SCC 345.

the answer appears relatively well settled now. A dominant platform's data practices can be subject of a Competition Commission proceeding; the appellate tribunal has so declared, and the fact that they also engage privacy considerations doesn't push them out of the Competition Commission's jurisdiction. Likewise, a dominant platform's data practices are something that the Data Protection Board can do something about because that is precisely its stated mandate. Each, individually, has the power to proceed against the same practices.

It isn't the regulators that create the problem. It is the space in between the regulators which the statute has left entirely vacant. There's no rule determining which regulator goes first. There's no prohibition on both pursuing the same conduct from the firm. There is no machinery through which they can be compelled to coordinate before taking action. What is invited to the empty space is the litigant, who will pick and choose the forum that serves them best, and contest those that do not. Instead of two regulators squaring off, one challenging the jurisdiction of the other, and the resulting fight necessarily having to be settled by a court, the phenomenon instead is one of subtler and more insidious forum shopping. Instead of the dispute turning on what the firm did, it depends on where the initial complaint was filed and how well a defendant argued it should have been somewhere else.

That, in the end, is the real state of the law. India has built two capable regulators and given each a sound reason to be interested in the same conduct. What it has not done is decide what should happen when both are interested at once. The choice this leaves is the familiar one between fixing the problem deliberately and waiting for the courts to fix it expensively. A sequencing rule, a principle against double punishment, and some agreed machinery for cooperation would not be difficult to enact, and they would spare the system a decade of the contradictory litigation that the last great jurisdictional overlap took to settle. The argument of this paper is not that the two regulators cannot coexist. It is that coexistence without a rule of priority is not really coexistence at all. It is an invitation, addressed to every well-advised litigant, to shop.

## References

[1] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[2] Competition Act, 2002 (Act 12 of 2003).

[3] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

[4] Competition Commission of India v. Bharti Airtel Ltd., (2019) 2 SCC 521.

[5] Coal India Ltd. v. Competition Commission of India, (2023) 10 SCC 345.

[6] In re: Updated Terms of Service and Privacy Policy for WhatsApp Users, Suo Motu Case No. 01 of 2021, Competition Commission of India, order dated 18 November 2024.

[7] WhatsApp LLC v. Competition Commission of India, Competition Appeal Nos. 1 & 2 of 2025, National Company Law Appellate Tribunal, judgment dated 4 November 2025.

[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[9] Law Commission of India and Ministry of Electronics and Information Technology, materials on the Digital Personal Data Protection framework.