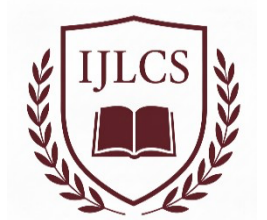


ARTICLE



DATA MARKETS AND STATE SURVEILLANCE: A COMPARATIVE CONSTITUTIONAL INQUIRY

Dipisha Chelani* and Ankit Singh Baghel**

Abstract

In the recent world personal data has become a strategic asset due to the quick development of the data markets and algorithmic governance, rapidly expanding the scope of state surveillance in constitutional democracies. This development raises a fundamental constitutional question that how should legal orders balance the demands the data-driven governance with ensuring the protection of fundamental rights most specifically, right to privacy in a political economy increasingly shaped by the data extraction and the logic of surveillance capitalism?¹

This paper conducts a comparative constitutional analysis of the India, Australia and the United States, to examine whether existing legal regulations have the structural potential to significantly limit the convergence between corporate data power and state authority. The analysis is intentionally placed within the larger political economy of data markets, emphasizing the institutional and democratic interests associated with these changes.

Although the Indian constitutional system has significantly recognized privacy as a fundamental right, demonstrates notable doctrinal dynamism, However the boundaries of this recognition are progressively being strained by massive state-run digital infrastructures. The Australian framework relies on legislative mechanisms that although flexible, are structurally vulnerable to executive overreach since it lacks an explicit constitutional guarantee. In United States, Fourth Amendment law which has long been seen as a pillar of privacy protection, is becoming more inadequate in addressing the dual pressure of widespread private sector data aggregation and digital surveillance.

In all three jurisdictions, due to the increasing coupling of public governance with surveillance capitalism has operated to normalize pervasive monitoring as a method of state administration. This paper examines that existing regulatory frameworks are not adequately equipped to address the governance realities brought about by the data driven power. As a result, it promotes the development of a renewed framework of digital constitutionalism, one that institutionalize strong data sovereignty as a foundational value and focuses on rigid mechanisms of democratic accountability within the governance of personal data.

Keywords – Data markets; State surveillance; Surveillance Capitalism; Right to privacy; Personal data protection; Data sovereignty; Digital Constitutionalism.

* Assistant Professor at Renaissance University, Indore.

** Assistant Professor at Renaissance University, Indore.

¹ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, New York, 2019).

I. Introduction

The recent growing digital technologies has changed the relationship between individuals' companies and the modern state. Today the digital Infrastructures are playing a drastic role as they are continuously focusing on every economic social and political life through collecting, processing and circulating personal information. Now the personal data or the information of an individual is not so personal it is available public through different digital systems. Every interaction with digital systems like biometric authentication, online communication, social media engagement, any financial transaction and digital welfare programs generate huge data which is capable of revealing the behavioral patterns of an individual. These patterns may involve personal preferences, relationships, and any social and political engagement. Therefore, the person has become a byproduct of technological interaction and acting as a resource of economic accumulation, administrative governance and political power.

Technology companies heavily depend upon the continuous extraction at and analysis of personal information for their profit generation. These technology companies require personal information for target advertising, Predictions, algorithmic profiling and optimum utilization of platform. This whole concept is termed as 'Surveillance capitalism', a practice in which human behavior is itself becomes a resource a source of commercial value.² Digital market is no more merely facilitating communication or market exchange but they are actually developing patterns of interaction consumption and decision making through different algorithmic systems through the data collection. This raised a serious concern regarding autonomy, transparency, democratic participation and accountability.

Not only private technology companies but governments in different constitutional democracies are now very much dependent on algorithmic technologies and large-scale databases to utilize them in areas such as welfare administration, policy making, taxation, funds Regulation, public health and national security. States are now dependent upon digital infrastructure and data driven governance systems. Digital public infrastructure initiatives, predictive governance tools, information retention and biometric identity systems are being offered more and more as ways to boost security coordination, reduce fraud and make efficient administration. However, these systems help in centralizing the information and monitoring the behaviors. So today the surveillance is not done solely by traditional methods but through interconnected structure involving both state institutions and private technology companies.

This change between governmental authority and corporate power creates hindrances in the individual's privacy. It creates a challenge that extends beyond the classical way of protection of privacy. Initially the constitutional structure was designed to regulate the states interference in private life. People rarely have understanding of the scope of data gathering, algorithmic processing and information exchange that takes place throughout the digital networks and meaningful consent is also a big challenge in the situations when using digital Platforms is practically required to obtain

² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs, New York, 2019).

public services, employment, banking, welfare benefits and communication networks. Therefore, the constitutional concern not just lies in the privacy violations but in the concentration of informational power within state institutions and private technological companies capable of shaping democracy itself.

Not just the above concerned issues this paper focuses on whether the existing constitutional framework and legal regulations have sufficient capacity to regulate the convergence between state surveillance and private data capitalism. It examines the comparative constitutional analysis of India, Australia and the United States jurisdiction specifically selected because they represent different constitutional approaches to govern the privacy of the individuals. In India we can see a model of rights-oriented constitutionalism in which Supreme Court has already recognized privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*, as and when the state expanded biometric governance through Aadhaar and digital welfare infrastructures.³ Australia represents statutory and administrative privacy system lacking exclusive guarantees, thereby creating the vulnerabilities of legal protections in executing surveillance and national security legislation. The United States constitutional system concentrated in Fourth Amendment protections against unreasonable searches and seizures but still lacking the system for platform surveillance, data collection and private sector data brokerage operating in the market beyond the control of traditional constitutional doctrine.

At glance, this paper focuses on comparative constitutional research informed by constitutional theories, political economy analysis and digital governance scholarship. It claims that existing privacy models are inadequate to address the contemporary systems of algorithmic governance and surveillance capitalism.

II. Surveillance Capitalism and the Data-Power Nexus

The concept of surveillance capitalism, systematically theorized by Shoshana Zuboff, provides the political economic foundation for this paper's analysis. Zuboff argues that a new economic logic has emerged, one that claims human experience behavior, emotion, location, social interaction as a free raw material, converts it into data, processes that data through sophisticated prediction algorithms, and sells the resulting 'behavioral futures' to advertisers and other actors who wish to influence future behavior.⁴ The most important aspect of this is, it works without the consent of the people whose information got extracted and it usually works in an opacity that actually resists the transparent constitutional governance.

Frank Pasquale's complementary concept of the 'black box society' draws attention to the opacity of the algorithmic systems through which surveillance capitalism operates. These systems are not only just for the profit generation or for the market but they are that powerful that they can affect the political power as well. The data which is being used for the targeted audience that same data is also affecting political micro targeting,⁵ Discriminatory credit assessment, predictive policy and the real

³ Justice K.S. Puttaswamy (Retd.) v Union of India, 2017 INSC 801 .

⁴ Ibid., ch. 1 ('Home or Exile in the Digital Future').

⁵ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, Cambridge, 2015).

time monitoring. Earlier the theories of state surveillance failed to anticipate that how the private data markets and the public governments will work together? Now they are not building its own surveillance infrastructure but they are dependent on the surveillance infrastructure private companies have built for their commercial purposes.

This combination of companies and state data power produces what this paper characterizes as the data-power nexus. This term emphasizes these structural configurations of corporate actors and the state authorities in surveillance mechanism, in which the purposes of their observation remain opaque.

III. Digital Constitutionalism and Data Sovereignty

Against the base of the data power Nexus this paper explains digital constitutionalism as its framework. Julie Cohen has described the central challenge as one of ‘informational capitalism as phase shift’: the emergence of data-driven, multi-dimensional commodification of social and economic life has so altered the structure of power that existing constitutional frameworks designed for an earlier phase of capitalist organization require fundamental reconception.⁶ Digital constitutionalism is not just the way the constitutional principles applied to the digital contexts but it is reconsidering the constitutional order for the transformation that digital infrastructure has produced in the organization of power.

Right now, three models of digital constitutionalism are in use. Firstly, the General Data Protection Regulation of the European Union which has developed a rights-based regulation in which GDPR functions as a quasi-constitutional instrument in which the individual rights are enforced, structural obligations on data processors are imposed and Independent supervisory structure is created.⁷ Secondly the Fourth Amendment’s protection against unreasonable searches and seizures. As the United States has always relied on negative liberty constitutionalism so through this Fourth Amendment’s protection, the primary constitutional safeguard is done. The Fourth Amendment’s protection maintains the constitutional privacy as freedom from government interference, which is actually not suits to regulate the private accumulation of data. Thirdly India’s developmental model which shows hybrid things like Privacy as a fundamental right merged with states over data infrastructure which is actually a threat to the right which it guarantees.

This paper focuses on data sovereignty not in its traditional international law sense but in its constitutional aspect. The focus is on the individual’s constitutionally guaranteed capacity to to exercise their personal data as a prerequisite for their democratic participation, human dignity and individual autonomy. Thus, data sovereignty is not just a regulatory framework but it is a foundational value or right that the state is obligated to protect.

⁶ Julie E. Cohen, ‘Informational Capitalism as Phase Shift: Challenges for Digital Constitutionalism’ in Giovanni di Gregorio, Oreste Pollicino & Peggy Valcke (eds), *Oxford Handbook of Digital Constitutionalism* (Oxford University Press, 2024); SSRN preprint: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4667197>.

⁷ Regulation (EU) 2016/679 (General Data Protection Regulation), Official Journal of the European Union, L 119/1, 4 May 2016. See also Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press, 2022).

IV. INDIA: CONSTITUTIONAL DYNAMISM UNDER STRUCTURAL STRAIN

Privacy as Fundamental Right

The development in India's constitution regarding privacy issues is held in the landmark judgment of *Puttaswamy (Retd.) v Union of India* (2017) 10 SCC. In this case, the bench held that the right to privacy is a fundamental right protected under article 14, 19 and 21 of the Indian Constitution.⁸ This judgment gave Privacy an important place in the right to life and personal liberty carrying human dignity and individual autonomy.

Through this case a concept came into existence which is now called as triple test for permissible state interference with the right to privacy. According to this test if state want to interfere in the privacy of an individual must satisfy three requirements namely – Legality, Legitimate , and Proportionality⁹

This case made a base in the Constitution for the protection of the privacy of individuals but it left with the actual legislative delivery. The application of this doctrinal achievement is still pending in the particular cases of state constructed digital infrastructure.

V. The Architecture of State Biometric Surveillance

The Aadhaar biometric identity system, operationalized under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, constitutes one of the most ambitious exercises in state data collection in any constitutional democracy.¹⁰ This system has onboarded billions of individuals through their fingerprints, iris and facial biometric data along with other information like demographic information to give them different benefits. This data is linked to different welfare benefits, financial services and encouraging state and private sector transactions. This structure is a perfect example of data power Nexus infrastructure that simultaneously gives the legitimate delivery to public services and a detailed surveillance of a population. The challenge to this Aadhaar was upheld by the constitutional validity to this Aadhaar Act by the bench in Justice K.S. Puttaswamy v Union of India (II) 2018 INSC 880 . This system clears the triple test which is set by the 2017 judgment.¹¹ And also ensures the legitimate aim of targeted welfare delivery. Although this case struck down the mandatory use of Aadhaar by private players in the market which says that biometric identification Used by the private sector will exceed the constitutional basis of the scheme.

This paper analyzes the limitation of the Aadhaar judgment in the purview of state data infrastructure. It argues it failed to require the government to demonstrate that less privacy-invasive alternatives to universal biometric identification had been considered and found inadequate; it deferred significantly

⁸ Justice K.S. Puttaswamy (Retd.) v Union of India, 2017 INSC 801 .

⁹ Ibid., para. 248 per Chandrachud J (majority). See also M.P. Sharma v Satish Chandra, District Magistrate, Delhi, MANU/SC/0018/1954; Kharak Singh v State of Uttar Pradesh, 1962 INSC 389 .

¹⁰ Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (Act No. 18 of 2016).

(the 'Aadhaar judgment').

to executive assessments of necessity; and it did not adequately engage with the systemic risks of function creep, the documented tendency of identification systems designed for welfare delivery to be repurposed for law enforcement, immigration control, and political surveillance.

VI. The Digital Personal Data Protection Act 2023

The evolution of Privacy Act of Data Personal Data Protection Act, 2023 became the India's first statutory data protection framework. This act adopts a different model and focuses on the specific requirements of the individual rights like the consent requirements over access, correction, and grievance redressal.¹² This act not only just focuses on the laws but also gives a platform for the people to get redressed from, the authority which primarily regulates the DPDPA, The Data Protection Board of India.

This act to genuinely solve the problems related to the privacy issues by the individuals in India and try to focus on the vacuum created by earlier regulations. However, there are three structural loopholes that Challenges the acts effectiveness. First, and most critically, Section 17 of the Act empowers the Central Government, by notification, to exempt any instrumentality of the State from all obligations under the Act where processing is 'in the interest of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence.'¹³ This exemption however created a broad independence add the legislative level which actually overlaps the state surveillance with Constitution's right to privacy. It has no independent judicial check.

Second, the Data Protection Board of India is appointed by, and answerable to, the Central Government. The Srikrishna Committee Report (2018) had specifically recommended that the appointment of the Data Protection Authority should involve the Chief Justice of India in the selection process, precisely to insulate it from executive control.¹⁴ This recommendation was given make the proper check in balance but this recommendation was not accepted. And because of this there is no effective check on the executive's data governance practices.

Third regarding the provisions regarding the children's data and the cross border transfers are solely dependent on the government Notifications that means the framework is still dependent on executive over certain matters.

In short DPDPA2023 solely focuses on the private sector with reasonable thoroughness while doesn't focus on the state actors which has major data dominance.

¹² Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Official text (India Code): <<https://www.indiacode.nic.in/handle/123456789/22037>>. The Digital Personal Data Protection Rules, 2025 were notified by MeitY on 13 November 2025 (Gazette of India Extraordinary, Part II, s.3(i), No. 843(E)).

¹³ DPDPA 2023, s. 17(2)(a). Compare Investigatory Powers Act 2016 (UK), s. 19 (judicial commissioner approval requirement).

¹⁴ Committee of Experts on Data Protection (Chair: Justice B.N. Srikrishna), 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians' (Ministry of Electronics and Information Technology, 27 July 2018), 151–152.

VII. AUSTRALIA: LEGISLATIVE FLEXIBILITY WITHOUT CONSTITUTIONAL ANCHOR

Australia's Constitution presents a different form of vulnerability. Unlike India in Australia there is no express bill or any express guarantee of privacy. The implied freedom of political communication recognised in *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106 is a structural implication of representative government, not a personal right; it does not extend to a general right of privacy.¹⁵

Because of this limitation the consequences are faced by the Australian people as they are entirely dependent on the legislative Majorities which either creates privacy protections or destroy or qualify them. There constitutional provision regarding the privacy which satisfy the rights related to privacy, there is no such coat which has this jurisdiction which can invalidate the legislation on the ground that it violates the privacy rights which gives rise to a constitutional gap at the center of Australia's privacy framework.

The Privacy Act 1988

The Privacy Act 1988 (Cth) and the thirteen Australian Privacy Principles (APPs) constitute the primary legislative framework for personal data protection in Australia. The Act applies to Australian Government agencies and to private sector organizations with an annual turnover exceeding AUD \$3 million (a threshold that excluded the majority of Australian businesses until recent reforms extended coverage from 1 July 2026).¹⁶ For the administration of this act the Office of the Australian Information Commissioner has been created which actually investigates and enforce the powers like initiating any civil proceeding or making any determinations. But this act also has some structural limitations which is been recorded in numerous cases.

Privacy Act Reform 2023–2025

Looking at the privacy regulations in Australia so many reforms were proposed and recommended regarding the Australia's privacy framework and some of them has been accepted and agreed and came into existence in the form of The Privacy and Other Legislation Amendment Act 2024. This act focuses on some serious issues like invasion of privacy, children's online privacy code framework, and Enhanced enforcement powers of the OAIC.¹⁷

Through the enactment of this act drastic changes came into existence and Australia seen genuine progress. The issues that were previously unavailable for the action are now became the right of the people, and they can now take the action against the infringement of their rights. Example serious privacy invasions which were earlier unrecognizable are now open for the actions. However these

¹⁵ *Australian Capital Television Pty Ltd v Commonwealth*, (1992) 177 CLR 106, 142 per Mason CJ.

¹⁶ Privacy Act 1988 (Cth). Current consolidated version: <<https://www.legislation.gov.au/Details/C2021C00139>>.

¹⁷ Attorney-General's Department, 'Privacy Act Review Report' (February 2023). Available at: <<https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>>. The Report contained 116 reform proposals.

reforms do not address the underlying constitutional vulnerability. These are legislative instruments depending on the legislative amendment by the same parliamentary majorities those enacted them.

In Australia's case a cyclic pattern of legislative adjustment is seen in privacy regulations that remain incapable of attaining true constitutional sufficiency in the absence of an entrenched constitutional basis. Although every turn of reform rectifies the errors revealed by the earlier one, but the legal system continues to operate without a constitutionally secured minimum available privacy protection.¹⁸

VIII. UNITED STATES: THE FOURTH AMENDMENT'S DIGITAL INADEQUACY

In United States from a very long time the basic Constitutional safeguard of the privacy in the digital age is Constitution's Fourth Amendment. The United States Constitution's Fourth Amendment states that the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. The execution and application of this amendment in the digital cases has been reduced due to a landmark case of *Smith v Maryland*, 442 US 735 (1979), which holds that information voluntarily disclosed to a third party carries no reasonable expectation of privacy and is therefore not constitutionally protected from government acquisition.¹⁹ But in today's digital world this doctrine is not sufficient, it produces a constitutional absurdity. Today the commercial intermediaries and technology companies are directly or indirectly controlling and recording all the person's life activities like location, communication, consumption, social interaction, political expression, sexuality etc. These details are recorded without the consent of the individuals and thus constitutionally unprotected from government acquisition.²⁰

Carpenter v United States (2018)

Carpenter v United States, 585 US 296 (2018)²¹ plays a significant role in the establishment of Third party doctrine. This case states that if government Acquires any Cell Site Location Information without the warrant keeps with it from seven or more days, then it comes under the search as per the Fourth Amendment. Cell Site Location Information is the part of the personal data gathered from the individuals without their consent the information like their location and their preferences. It helps the government to achieve near perfect surveillance through acquiring the detailed encyclopedia with the effortless compilation of the data which automatically generated without any positive of the user. It can help the government to travel in the past and collect the information of a person and reveal the privacies of life.

The *Carpenter* decision is, however, explicitly and deliberately narrow. Chief Justice Roberts emphasized that the holding applied only to historical CSLI acquired over an extended period; it did

¹⁸ Senate Estimates hearing, Attorney-General Michelle Rowland, 10 February 2026 (Tranche Two reforms in preparation). See Salinger Privacy, above n 18.

¹⁹ *Smith v Maryland*, 442 US 735, 744 (1979) (Stewart J for the Court).

²⁰ See Orin S. Kerr, 'The Case for the Third-Party Doctrine' (2009) 107 Michigan Law Review 561 (defending); Neil Richards, *Why Privacy Matters* (Oxford University Press, 2022), ch. 5 (critiquing).

²¹ *Carpenter v United States*, 585 US 296 (2018). Official opinion: <https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf>.

not address real-time CSLI, other categories of digital business records, the acquisition of data from sources other than telecommunications providers, or any collection technique involving foreign affairs or national security.²² The main concern in which the personal data is pervasively and involuntarily recorded unaddressed by this case.

The Commercialization of Surveillance: Data Brokers and the Constitutional Vacuum

With the emerging digital market, the commercial data brokers have exploded in the market. These data brokers are the industries or the companies that collect the personal data from public records, Company transactions, social media interference and surveillance infrastructure and trade in those individual profiles with government and private purchasers. And this concern is remained untouched from the fourth Amendment.

Multiple federal agencies, including components of the Department of Homeland Security, the Internal Revenue Service, and the Department of Defense, have been documented purchasing location data, social media data, and demographic profiles from commercial brokers, circumventing the warrant requirement entirely because the government is not ‘accessing’ third-party records but purchasing data on the open market. Through the US framework we can say that the major threat is not the state-built surveillance infrastructure but the privatization of surveillance itself. The constitutional framework does not reach the problem of outsourcing data collection from the private sectors.²³

IX. COMPARATIVE SYNTHESIS: THREE JURISDICTIONS, ONE STRUCTURAL PATHOLOGY

Through the comparative analysis of these three jurisdictions, we can say that despite of having substantial differences in the constitutional architecture, there are some major loopholes in protecting the personal rights over the digital platform. A common structural problem is identifiable in each of three cases. In all the three cases we can see that the increase in the public governance with the infrastructure of surveillance capitalism with the pervasive monitoring as a routine method of administration where the legal framework is still incomplete or inadequate to address this normal and make it a meaningful constitutional constraint.

In India this problem can be seen in a way the constitutional right to privacy is there with the legislative design but still lacks executive procedures and coexisting the right in practice. The const Thomas is genuine but the internal structure is still weak. In Australia’s case the constitution is mute, and completely depends upon the will of the legislative body where the political environment strongly influences the privacy related concerns. In United States the problem of commercialization of surveillance is a major loophole in the structure set up by the fourth Amendment, which gives a

²² Ibid., 316 (Roberts CJ explicitly noting the narrowness of the holding).

²³ See Electronic Frontier Foundation, ‘Government Purchase of Data from Data Brokers’ (EFF, 2023): <<https://www.eff.org/issues/privacy>>; FTC, ‘Commercial Surveillance Advanced Notice of Proposed Rulemaking’ (August 2022): <<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/08/commercial-surveillance-advanced-notice-proposed-rulemaking>>.

way to the state data acquisition through the different market players and the amendment is unable to regulate these problems.

There are some common things which can be identified in three these three state's analysis- First in all the three jurisdictions the major actor which is responsible for the data governance are the executive agencies not the constitution and not even the judiciary. Second the use of the personal data is more from the state sector rather than the private sector and then too we do not have any privacy regulation which focuses on this coercive practice. Third in all three jurisdictions there is no proper structure which is or institutionalized to oversight the systematic exercise of state data and genuine efforts to protect democracy.

X. TOWARDS DIGITAL CONSTITUTIONALISM: A RENEWED FRAMEWORK

With the comparative analysis developed in the previous sections of this paper, the need of a proper framework is proposed. A structure through which digital constitutionalism will be protected and the governance should be smooth enough to cope up with the challenges of the contemporary data economy.

This can be by considering three things first the constitutional framework of data sovereignty. Through this framework the individual will get a guaranteed to be informed and exercise meaningful control over his or her personal data. The framework should have that constitutional value which not merely just a legislative 1 but if it infringed the person get redressed through the judiciary. By analyzing the three jurisdictions in this paper we can see the legislative privacy is however sophisticated but structurally weak and suppressed through the same majoritarian pressure those who exercising the expansion of surveillance state.

The second requirement is the institutional independence of data governance structure. The data protection authorities must be protected from executive influence not only at the base level but deep rooted through structural safeguards. This can be done through the appointment procedures that involve judicial or legislative participation instead of exclusive executive discretion, The removal should be permissible only on specific grounds and open to judicial scrutiny and financial autonomy should be assured.

The third important element is democratic oversight with the framework of data governance . This can be done through the creation of structured processes through which elected bodies are able to supervise, evaluate and scrutinize the states data collection and deployment of data in an informed manner. This will require significant surveillance initiatives undertaken by the state, public authorities regularly disclose the information regarding the data, the civil society groups should be granted participatory rights in regulation and policy making processes related to data governance.

XI. CONCLUSION

This paper has conducted a comparative analysis of the data surveillance and privacy protection in India, Australia and United States. The purpose behind conducting this research was whether the

existing legal regulations have the capacity to meaningfully constrain the convergence of Surveillance Capitalism and State Authority. The analysis says that they do not. These frameworks which are in existence are made for the world in which States data gathering capacities were limited by practical constraints and not affected by the infrastructure of global data markets. These frameworks were sufficient when the boundary between corporate power and state power was sufficiently clear to make independent regulation.

But the data economy has now made these assumptions obsolete. The convergence of corporate data infrastructure and state governance has now proved that these structures are beyond the reach of frameworks already made. India's traditional way of constitutional adaptability is being undermined by its own digital systems created and operated by state itself. In Australia the continuous change in the legislations and frameworks make the laws incapable of achieving real constitutional sufficiency. And in the United States due to the expansion of surveillance practices the protections given under fourth Amendment became weak.

Through the analysis the proposal is the making of new framework for digital constitutionalism in the shadow of constitutional entrenchment of data sovereignty, insulation of data governance and strong structure of democratic accountability is required. The present conference, bringing together comparative constitutionalists from common law and civil law traditions across three continents, is precisely the forum in which the transnational dialogue required for this project of constitutional renewal can begin.