Designed to Serve Mankind? The Politics of the GDPR as a Global Standard and the Limits of Privacy

Roxana Vatanparast[*]

Abstract

Data collection and processing have been subject to considerable controversy in recent years, sparking many debates and governance projects. One such governance project is the General Data Protection Regulation (GDPR). Since becoming effective, the GDPR has come to represent a "global standard" for privacy and data protection. Yet, the idea that the GDPR represents a global standard overlooks broader questions about the interaction between law, technology, and society.

Using co-production as a conceptual lens, this paper argues that the GDPR reflects at least three social shifts, each of which is entangled with

[*] Visiting Fellow, Program on Science, Technology and Society (STS Program) at Harvard Kennedy School; PhD, University of Turin; JD, UC Hastings College of the Law. This article benefitted from comments by *Elettra Bietti*, *Sheila Jasanoff*, *Jhalak Kakkar*, *Luisa Scarcella*, and the Fellows of the STS Program. I would like to thank them for their insightful comments. I would also like to express my gratitude to the STS Program, the Institute for Global Law & Policy at Harvard Law School (IGLP), and the University of Turin for institutional support during the writing of this article.

the others. Along with these social shifts, the GDPR is also co-producing ideas of what privacy is and ought to be, and who gets the authority to interpret and construct it. Moreover, the GDPR reconstructs political subjects into data subjects, with significant depoliticising and disempowering effects. Ultimately, the GDPR does more to serve the interests of informational capitalism than to challenge it. Locally situated political engagement can provide a way to counter the disempowering effects of the GDPR as a global standard for marginalised people in the Global South, as this article explores in the context of India's new data protection bill.

I. Introduction

The collection and processing of our personal data are changing sense-making of the world and of ourselves, as are projects of governance surrounding them. Data collection and processing have been subject to considerable controversy in recent years, sparking many debates and governance projects around how to best promote the social good in light of technological developments that have enabled the scale of these practices to greatly increase. In turn, these developments have enabled increased concentration of power in the hands of those who play significant roles in commodifying and controlling the use of personal data – namely, technology corporations and the people behind them.

One such governance project is the General Data Protection Regulation (Regulation (EU) 2016/679). Since becoming effective, the GDPR has come to represent a "global standard" for privacy and data protection for some.[1] According to the European Commission, for example, the GDPR "has emerged as a reference point and acted as a catalyst for many countries and

[1] See, *e.g.* European Commission, Joint Statement by First Vice-President *Timmermans*, Vice-President *Ansip*, Commissioners *Jourová* and *Gabriel* ahead of Data Protection Day, STATEMENT/19/662 (Brussels, 25.1.2019), available at: <http://europa.eu> (last visited 19.5.2019); *B. A. Safari*, Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection, Seton Hall Law Review 47 (2017), 809; *E. Schulze*, Microsoft CEO Satya Nadella: Tech Companies Need to Defend Privacy as a Human Right, CNBC, 1.11.2018, <https://www.cnbc.com> (last visited 19.5.2019). Some scholars, however, contends that the GDPR is not setting a global standard due to the development of competing privacy regulatory regimes and models. See, *e.g. S. Togawa Mercer*, Symposium on the GDPR and International Law: The Limitations of European Data Protection as a Model for Global Privacy Regulation, AJIL Unbound 114 (2020), 20; *A. Chander/M. E. Kaminski/W. McGeveran*, Catalyzing Privacy Law, Georgetown Law Faculty Publications and Other Works. 2190 (2019), <https://scholarship.law.georgetown.edu> (last visited 26.11.2019).

states around the world considering how to modernise their privacy rules", noting that there is a global convergence in several jurisdictions' initiatives and international instruments that are based on principles shared with the GDPR.[2] The United Nations (UN) Secretary General *António Guterres* has stated that the GDPR has "set an example [...] inspiring similar measures elsewhere" and "urge[d] the EU and its Member States to continue to lead to shape the digital age and to be at the forefront of technological innovation and regulation".[3]

Yet, the idea that the GDPR represents a global standard assumes a uniform cultural, political, and economic context globally and overlooks broader questions about the interaction between law, technology, and society. Indeed, an alternative view might illuminate how the GDPR's individual privacy and data protection framework derives from a particular political and cultural context, embedding, prioritising, and stabilising certain political claims and values over others.

The potential multiplicity of legal regimes governing data privacy and transfers of personal data has raised concerns about the fragmentation of the internet as a result of clashing regulatory regimes and normative orders and the potential rise of borders in cyberspace.[4] In light of this concern, some propose that the GDPR become a global standard in order to avoid such conflicts and the resulting effects they might have, such as creating conflicting obligations for collectors and processors of personal data, as well as uneven levels of data protection for people located in different jurisdictions. Despite these concerns, there have been surprisingly few actual conflicts between different legal regimes surrounding data flows.[5]

Here the concept of co-production developed by *Sheila Jasanoff* is particularly useful to examine the interconnections between the GDPR, personal data processing, and the social.[6] Co-production refers to the idea that "the ways in which we know and represent the world (both nature and so-

[2] European Commission, Two Years of the GDPR: Questions and Answers, European Commission, <https://ec.europa.eu> (last visited 29.8.2020).

[3] Address of the UN Secretary-General to the Italian Senate, 18.12.2019, available at: <https://www.un.org>.

[4] *D. R. Johnson/D. G. Post*, Law and Borders—The Rise of Law in Cyberspace, Stanford L. Rev. 48 (1996), 1367.

[5] *S. Humphreys*, Data: The Given, in: J. Hohmann/D. Joyce (eds.), International Law's Objects, 2019 (citing *C. Kuner*, Transborder Data Flows and Data Privacy Law, 2013).

[6] *S. Jasanoff*, The Idiom of Co-Production, in: S. Jasanoff (ed.), States of Knowledge: The Co-Production of Science and the Social Order, 2004, 1 et seq.

ciety) are inseparable from the ways in which we choose to live in it".[7] In this view, technology

> "both embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments and institutions – in short, in all the building blocks of what we term the *social*".[8]

Through this analysis, it emerges that the GDPR reflects at least three social shifts, each of which is entangled with the others. First, the GDPR marked a practical shift in data collection practices, at the technological and institutional levels. Second, the GDPR represented a stabilisation of the public discourse on personal data collection and processing around the issue of privacy, a discourse which became institutionalised through the GDPR, as well as the adoption of similar measures and language by other jurisdictions and institutions. This discursive stabilisation in turn has effects on collective understandings and framings of the problems surrounding data processing, reflecting also an epistemological stabilisation. Third, the GDPR elevated the privacy rights claims of certain subjects, namely individual "data subjects" in the European Union (EU), reflecting a normative shift. This normative shift not only prioritises individual privacy rights *vis-à-vis* data collection, but also raises questions as to who gets to have those rights and who has the authority to make those decisions. In doing so, it overlooks other important considerations and social problems that arise in connection with data collection.

Along with these social shifts, the GDPR is also co-producing ideas of what privacy is and ought to be, and who gets the authority to interpret and construct it. While it provides mechanisms for "legitimate" ways of governing the processing of personal data and checklists for companies concerned with regulatory compliance, it does little to question power dynamics and asymmetries underlying the relationships between technology corporations and individual people. Indeed, according to *Fleur Johns*,

> "there is much more at issue in the governance of the emerging global data economy than technical interface between existing legal systems and well-aired privacy concerns".[9]

Moreover, in contributing to the social shifts and power dynamics outlined here, the GDPR reconstructs political subjects into data subjects, with

[7] *S. Jasanoff* (note 6), 2.
[8] *S. Jasanoff* (note 6), 3.
[9] *F. E. Johns*, The Deluge, London Review of International Law 1 (2013), 9, 14.

significant depoliticising and disempowering effects. The GDPR, by being premised on liberalism's elevation of individual rights, results in depoliticisation, or the removal or displacement of political concerns to ostensibly non-political, technical, and neutral domains.[10] The GDPR, as power-knowledge, ultimately does more to serve the interests of informational capitalism[11] than to challenge it. Locally situated political engagement can provide a way to counter the disempowering effects of the GDPR as a global standard for marginalised people in the Global South,[12] as this article explores in the context of India's new data protection bill.

II. The GDPR as Power-Knowledge

The GDPR is not just a data protection regulation. It is also acting as a tool of governance of populations and economic activity. Data protection under the GDPR constitutes the exercises of power along the three axes that *Foucault* described as a "dispositive of power" – namely, the formation of sciences around it, systems of power to regulate its practices, and ways in which individuals come to recognise themselves as its subjects.[13] The GDPR requires experts such as lawyers, scholars, judges, supervisory authorities, the European Data Protection Board, and technologists to interpret and co-construct it, it can rely on courts such as the Court of Justice of the European Union (CJEU) to enforce its provisions as well as the EU's own regulatory and market power to generate compliance outside the EU, and it transforms political subjects into data subjects. In doing so, the GDPR has be-

[10] On depoliticisation in relation to liberalism, see *C. Schmitt*, The Concept of the Political, (*George Schwab* trans., 2007).

[11] I follow *Julie Cohen's* definition of informational capitalism here to refer to a regime where "market actors use knowledge, culture, and networked information technologies as means of extracting and appropriating surplus value, including consumer surplus". *J. E. Cohen*, Between Truth and Power: The Legal Constructions of Informational Capitalism, 2019, 6.

[12] *P. Arora*, General Data Protection Regulation – A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South, Surveillance & Society 17 (2019), 717.

[13] On the "dispositive of power" in relation to how power is exercised over sexuality, see *M. Foucault*, The History of Sexuality, Vol. 2: The Use of Pleasure 4 (*Robert Hurley* trans., 1985). While sociologist *S. Coll* makes this argument with regard to privacy more generally, this article focuses more specifically on the GDPR. See *S. Coll*, Power, Knowledge, and the Subjects of Privacy: Understanding Privacy as the Ally of Surveillance, Information, Communication & Society 17 (2014), 1250.

come the site of power-knowledge,[14] where privacy and data protection can be used as tools to help serve the interests of informational capitalism rather than challenge it.[15] To properly challenge the business models at the heart of informational capitalism, more would be needed than privacy and data protection. By using knowledge practices of the law, the GDPR as a global standard might limit democratic decision-making with regard to sociotechnical practices such as data collection, processing, and analytics. It attempts to define what privacy and data protection are and it undemocratically delegates authority for interpreting what they should be and how they should be implemented.

These power dynamics should be placed within the context of economic globalisation that has simultaneously challenged public global normativity, and motivated governance projects at the global scale. The EU as a global standard setter reflects its role as a post-national liberal realist power, where it must contend with both strong states, such as China and the United States (US), and non-state actors, such as corporations involved in creating private global normative orders.[16] Global standard setting by the EU through the GDPR and its extraterritorial provisions is one such exercise of power.

Further, uniform global standards for data protection, like international law's universalising tendency, tend to ignore uneven development and the material and economic conditions of the third world.[17] In international legal scholarship, scholars have critiqued international law and its institutions in imposing policies and laws that originate in the Global North on the Global South.[18] In the process, they undermine democracy and often legitimise neoliberal policies that perpetuate domination and structural global inequalities.[19] The universalisation of laws that are locally produced can have anti-

[14] See, *e.g. M. Foucault*, The History of Sexuality, Vol. 1: An Introduction (Reissue ed. 1990); *M. Foucault*, "Society Must Be Defended": Lectures at the Collège de France, 1975-1976, 252 (*David Macey* trans., 2003).

[15] On this argument in relation to privacy, see *S. Coll* (note 13).

[16] On liberal realism structuring the EU, see *A. Skordas*, The European Union as Post-National Realist Power, in: S. Blockmans/P. Koutrakos (eds.), Research Handbook on the EU's Common Foreign and Security Policy, 2018, 394 et seq.

[17] On this argument in relation to international law, see *B. S. Chimni*, Third World Approaches to International Law: A Manifesto, International Community Law Review 8 (2006), 3 et seq.

[18] *B. S. Chimni*, International Institutions Today: An Imperial Global State in the Making, EJIL 15 (2004), 1 et seq.; *B. S. Chimni* (note 17).

[19] *B. S. Chimni* (note 17).

democratic and distributive effects that should be taken into account.[20] To counter international law's tendency to universalise and impose on the Third World, scholars have suggested amplifying the concerns, engagements, and voices of Third World peoples.[21]

III. Background on GDPR

The GDPR, passed by the European Parliament on 27.4.2016 and made applicable on 25.5.2018, was intended to replace the Data Protection Directive 95/46/EC (DPD), harmonise regulation of data protection in the EU, protect EU citizens' fundamental rights, and change the way organisations and companies treat data privacy.[22] The European Commission proposed strengthening online privacy rights by reforming the DPD in 2012, as the DPD was thought to be outdated in a time when the data collection practices of organisations had vastly changed in scope and volume since 1995.[23] The main aim of the GDPR was framed in terms of fundamental rights and data protection, but also regulating the free movement of data in the digital economy and in the internal market.

The GDPR vastly expanded the territorial scope of application as compared to the DPD. The GDPR applies to data controllers and processors established in the EU, regardless of whether the processing takes place in the EU.[24] Article 3 and Recitals 22-25 of the GDPR provide that the regula-

[20] Scholars such as *Sornarajah* and *Schneiderman*, for example, have discussed how US standards became global standards in the realm of international economic law through investment protections that became the normative and legal standard around the world. In the international economic law context, they describe how the globalisation of the locally situated investment rules had anti-democratic and distributive effects – distributive both in terms of distributing economic wealth and in terms of the power to set normative economic standards being in the hands of the United States. See, *M. Sornarajah*, The Case Against a Regime for International Investment Law, in: L. E. Trakman/N. W. Ranieri (eds.), Regionalism in International Investment Law, 2013; *D. Schneiderman*, Constitutionalizing Economic Globalization: Investment Rules and Democracy's Promise, 2008.

[21] *B. Rajagopal*, International Law from Below: Development, Social Movements and Third World Resistance, 2003; *B. S. Chimni* (note 17); *S. Pahuja*, Decolonising International Law: Development, Economic Growth and The Politics of Universality, reprint ed. 2013.

[22] Regulation (EU) 2016/679, of the European Parliament and the Council of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) [hereinafter GDPR].

[23] GDPR (note 22), Recital 6.

[24] GDPR (note 22), Art. 3(1).

tion also applies to non-EU based organisations if they process the data of EU data subjects in connection with offering goods or services to individuals in the EU or monitoring their behaviour in the EU.[25]

The GDPR's extraterritorial reach might imply efforts to set standardising norms with universal effects.[26] The EU's history and power (both political and economic) has a great deal to do with why the GDPR's extraterritoriality has actually had such a strong impact – a function of its willingness to assert its regulatory power outside its own borders and its ability to wield its power to generate those effects elsewhere.[27] This is due in part to the EU's market power, which it can use to assert its normative authority beyond its borders.[28] Had the GDPR been adopted with the same provisions, language, and extraterritorial reach in a jurisdiction with less power and influence than the EU, it likely would not yield the same effects.[29]

The next sections will discuss the legislative history of the GDPR as well as its provisions and case law. These show that the GDPR prioritises data protection and the closely linked idea of individual privacy, as can be seen in its provisions, as well as in its implementation and interpretation.

1. Legislative History

Some scholars have attributed the GDPR's origins to the US Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems' Report issued in 1973 titled "Records, Computers, and

25 GDPR (note 22) Art. 3(2).

26 *C. Ryngaert*, Whither Territoriality? The European Union's Use of Territoriality to Set Norms with Universal Effects, in: C. Ryngaert/E. J. Molenaar/S. M. H. Nouwen (eds.), What's Wrong with International Law?, Liber Amicorum A. H. A. Soons, 2015, 434 et seq.

27 *D. Kennedy*, A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy, 2018, 211.

28 For example, *Saluzzo* notes that the EU is a global standard-setting actor, as it is able to effectively set normative standards extraterritorially through adequacy assessments for data transfers to outside the EU. See *S. Saluzzo*, The EU as a Global Standard Setting Actor: The Case of Data Transfers to Third Countries, in: E. Carpanelli/N. Lazzerini (eds.), Use and Misuse of New Technologies, 2019, 115 et seq.

29 This is not to ignore different regulatory and policy approaches that do exist. While China and the US could be considered exceptions to this with their different approaches to data transfers, data protection, and privacy, the extraterritorial effects of the GDPR mean that organisations that fall within its scope must comply with it, wherever they are located. The GDPR's extraterritorial effects likely would not have easily been achieved by all regulators without normative authority on the level of the EU.

the Rights of Citizens",[30] Fair Information Practices (FIPs), and the Privacy Act of 1974.[31] Others attribute its origins to developments in the EU, such as data protection laws in Sweden,[32] the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980),[33] the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981),[34] and the DPD, which set the stage for the eventual development and framing of the GDPR's provisions relating to data protection. As reflected in these instruments, from 1980 onward, the European regulatory approach with regard to personal data has been to protect the fundamental right of privacy and the closely associated fundamental right of personal data protection for individuals.[35] Convention 108, for example, had the objective of ensuring

> "for every individual […] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')".[36]

---

[30] *P. Pałka*, Data Management Law for the 2020s: The Lost Origins and the New Needs, Buff. L. Rev. 68 (2020), (citing U.S. Department of Health, Education & Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records Computers and the Rights of Citizens (July 1973) [hereinafter 1973 Report]). *Pałka* also traces how the American approach to data privacy can also be traced back to this report, but of course took on a different trajectory, with the American approach "favoring the markets, self-regulation and individual choice […]." *P. Pałka* (note 30), 6.

[31] *C. J. Hoofnagle/B. van der Sloot/F. Zuiderveen Borgesius*, The European Union General Data Protection Regulation: What It Is and What It Means, Information & Communications Technology Law 28 (2019), 65, 70.

[32] Sweden, Data Act of 1.5.1973, available at: <https://resources.law.cam.ac.uk> (last visited 10.9.020); *B. van der Sloot*, Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation, International Data Privacy Law 4 (1014), 307.

[33] Ministerial Council of the Organization for Economic Cooperation and Development, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Doc. C(80)58/FINAL, 23.9.1980, available at: <https://www.oecd.org> [hereinafter 1980 OECD Guidelines].

[34] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series – No. 108, 28.1.1981, available at: <https://www.coe.int> [hereinafter Convention 108].

[35] *P. Pałka* (note 30), 16 (citing *G. Gonzalez Fuster*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014).

[36] See note 34.

In 2000, Article 8 of the EU Charter of Fundamental Rights recognised the fundamental right to protection of personal data, and Article 7 recognised the fundamental right to privacy.[37]

Some of these earlier guidelines and directives contained similarities with the 1973 Report.[38] Unlike the 1973 Report, however, these instruments eliminated the public deliberation aspect of privacy, or in other words, the idea that privacy also encompassed the participation of individuals and the public in deciding how their data should be used.[39] These instruments moved away from the 1973 Report's public disclosure requirements and instead required individual data protection. The GDPR, building on these prior guidelines and directives, reflects a liberal, individualistic ideology of privacy.[40] It is premised on a human rights, or fundamental rights, framework prioritising individual rights to privacy and data protection, themselves built on liberal notions of individual autonomy, freedom, and the distinction between private and public spheres of life.[41] In protecting the rights of data subjects, the GDPR reflects a trend toward increased focus on the individual at the heart of data protection rules.[42]

The GDPR provides technocratic solutionism for protection of individual interests over and above collective interests and political remedies.[43] This bias toward individual privacy rights in the GDPR is also evident in the provisions of the GDPR, as well as recent CJEU case law interpreting data protection laws, including both the DPD and the GDPR.

2. Provisions and Case Law

The GDPR states that one of its objectives is to protect "fundamental rights and freedoms of natural persons and in particular their right to the

[37] See Charter of Fundamental Rights of the European Union, OJ C326/1, 26.10.2012, 391 et seq. [hereinafter the EU Charter]. In 2009, the Lisbon Treaty granted the EU Charter legally binding force. See Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon [2007] OJ C306/1.

[38] *P. Pałka* (note 30), 11 et seq.

[39] *P. Pałka* (note 30), 12.

[40] On the liberal individualist roots of privacy theory (especially in US legal scholarship), its notion of the autonomous liberal self, and its limitations, see *J. E. Cohen*, What Privacy Is For, Harv. L. Rev. 126 (2013), 1904, 1906 et seq.

[41] *P. Pałka* (note 30), 16; *G. Gonzalez Fuster* (note 35), 22 et seq.

[42] *B. van der Sloot* (note 32), 307.

[43] *P. Pałka* (note 30), 16.

protection of personal data".[44] Data protection and privacy effectively go hand in hand in EU law,[45] even if data protection often refers to "a set of norms that serve a broader range of interests than simply privacy protection".[46] The individualised aspect of the GDPR can be inferred from many of the provisions of the regulation with regard to data subjects' rights, such as consent as a basis for lawful processing of personal data,[47] right of access,[48] right to rectification,[49] right to erasure,[50] right to restriction of processing,[51] right to data portability,[52] and the right to object.[53]

The CJEU has taken an especially protective stance with regard to data privacy in the aftermath of the *Edward Snowden* revelations on US government surveillance.[54] In 2015, for example, the CJEU invalidated the Safe Harbor Agreement governing data transfers between the US and EU, on the basis that it did not offer adequate protection against government surveillance.[55]

Moreover, the CJEU has interpreted data protection regulations like the DPD (the GDPR's predecessor) as intending to protect the right to privacy. In the *Wirtschaftsakademie* case, the Court ruled that Facebook Page administrators are joint controllers, and thus, share responsibility to ensure compliance with data protection laws.[56] This is so even if they do not control or have access to the personal data collected through their Facebook Page and only have access to aggregated or anonymised data.[57] In taking its decision, the Court highlighted that the purpose of data protection and regulations on processing of personal data is to ensure fundamental rights, es-

---

[44] GDPR (note 22), Art. 1.

[45] *G. Gonzalez Fuster* (note 35), 5, 75 et seq.

[46] *L. A. Bygrave*, Privacy and Data Protection in an International Perspective, Scandinavian Studies in Law 56 (2010), 165, 168.

[47] GDPR (note 22), Arts. 6, 7, 9.

[48] GDPR (note 22), Art. 15.

[49] GDPR (note 22), Art. 16.

[50] GDPR (note 22), Art. 17.

[51] GDPR (note 22), Art. 18.

[52] GDPR (note 22), Art. 20.

[53] GDPR (note 22), Art. 21.

[54] *M. Zalnieriute*, International Decisions: Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), AJIL 114 (2020), 261, 265.

[55] *Maximillian Schrems v. Data Protection Commissioner*, ECJ Case C-362/14, 6.10.2015.

[56] *Wirtschaftsakademie Schleswig-Holstein GmbH v. Facebook Ireland Ltd*, ECJ Case C-210/16, 5.6.2018, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht [hereinafter *Wirtschaftsakademie*]. Since the definition of "controller" is identical in the DPD and the GDPR, this case is also relevant for determining responsibility for compliance with the GDPR.

[57] *Wirtschaftsakademie* (note 56).

pecially the right of privacy, as enshrined in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of EU law.[58]

Moreover, while the CJEU ruled in 2019 that the "right to be forgotten" under EU law only requires de-referencing on websites accessible in EU member states, it left open the possibility for member states to order global removal of search results. In 2014, the CJEU established the "right to be forgotten" on the basis of Articles 12 and 14 of the DPD.[59] Article 17 of the GDPR has also incorporated the right to be forgotten, but it did not contain express terms as to its territorial reach. In the *Google LLC v. CNIL* case, Google challenged the Commission Nationale de l'Informatique et des Libertés' (CNIL) imposition of a €100,000 fine for violation of the right to be forgotten for only removing search results accessible in EU member states. The CJEU found that it could not impose EU legislation beyond member states, and left ambiguous whether "geo-blocking" techniques, or preventing users located in certain jurisdictions from accessing search results, were sufficient to comply with the right to be forgotten.[60] It also left open the possibility for member states to order global removal of search results. This indicates that the GDPR allows for wide discretion by member states, even if the GDPR and the DPD did not explicitly confer extraterritorial scope to the right to be forgotten.[61] This result is also indicative of the CJEU's hard-line stance on data privacy, as it allows room for member states to apply stronger protections for data privacy than the express provisions of the GDPR, even if that risks going against the GDPR's aim of harmonisation across the EU.[62]

Finally, *Schrems* filed another case with the CJEU (*Schrems II*) which sought to invalidate the EU-US Privacy Shield as well as EU Standard Contractual Clauses (SCCs) that are used by companies like Facebook to legitimise cross-border transfers of data between the EU and the US.[63] In its decision, the CJEU invalidated the Privacy Shield as a means to transfer per-

58 *Wirtschaftsakademie* (note 56).

59 *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, ECJ Case C-131/12, 13.5.2014 [hereinafter *Google Spain*]. See also *M. Zalnieriute* (note 54), 261 et seq.

60 *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*, ECJ Case C-507/17, 24.9.2019) [hereinafter *Google LLC v. CNIL*].

61 See *Google LLC v. CNIL* (note 60); *M. Zalnieriute* (note 54), 263.

62 *M. Zalnieriute* (note 54), 266.

63 *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* [hereinafter *Schrems II*], Case C-311/18, Reference for a Preliminary Hearing from the High Court (Ireland), 9.5.2018), available at: <http://curia.europa.eu> (last visited 30.8.2020).

sonal data to the US, and held that SCCs are insufficient for data transfers to the US without additional protections against surveillance.[64] In this case, the CJEU again reiterated its strong protection of data privacy rights over other interests. Moreover, the CJEU's record of invalidating adequacy frameworks of the EU with the US in *Schrems I* and *Schrems II* leaves "little room for manoeuvre in accommodating third party norms".[65]

These cases illustrate the CJEU's consistent prioritisation of the right to data protection and the right to privacy over other interests, such as security and free movement of information.[66] This interpretation is consistent with the underlying objectives of the DPD and the GDPR to prioritise the fundamental rights of data protection and privacy.

IV. The Three Social Shifts

1. The Technological and Institutional Shift

Although the GDPR was adopted partly in response to changes in technologies that permitted the collection and analysis of massive datasets,[67] or so-called "big data", the regulation has also changed the technological and institutional practices in the aftermath of its implementation on 25.5.2018. Indeed, the idiom of co-production refers to the idea that technologies are shaped by, embed, and in turn help shape, social, economic, and political orders.[68] Technologies therefore embed and shape social contexts, including legal orders.

For example, in response to the GDPR, some technology companies moved user data off of EU servers,[69] changed their advertising practices on their websites in the EU,[70] and certain websites were blocked in the EU,[71]

---

[64] *Schrems II* (note 63), Judgement of the Court, 132 et seq., 168, 199 et seq., 1.7.2020, available at: <http://curia.europa.eu> (last visited 30.8.2020).

[65] *C. Kuner*, The Schrems II judgement of the Court of Justice and the Future of Data Transfer Regulation, European Law Blog (2020), available at: <https://europeanlawblog.eu> (last visited 30.8.2020).

[66] *C. Ryngaert/M. Taylor*, The GDPR as Global Data Protection Regulation?, AJIL Unbound 114 (2020), 5 et seq.

[67] GDPR (note 22), Recital 6.

[68] *S. Jasanoff* (note 6), 1.

[69] *A. Hern*, Facebook Moves 1.5bn Users Out of Reach of New European Privacy Law, The Guardian, 19.4.2018, <https://www.theguardian.com> (last visited 7.9.2019).

[70] Changes to Our Ad Policies to Comply with the GDPR, Google, 2018, <https://www.blog.google> (last visited 7.9.2019).

reflecting changes in the technological practices. Moreover, as a result of the GDPR, some platforms stopped obtaining or sharing data with third party data brokers and increased interoperability between platforms.

As separating out personal data belonging to EU data subjects from those of others can be technically burdensome, many technology corporations have implemented changes to accommodate the EU's data protection regime across the board for all of their users, to reduce the burden of having to comply with multiple regulatory regimes.[72] Microsoft, for example, announced that it would "extend the rights that are at the heart of GDPR to all of our consumer customers worldwide".[73]

Moreover, the GDPR has required technology companies to respond directly to requests from EU data subjects for access and information[74] on the types of personal data collected on them and for what purposes, to requests for deletion of links to web pages that result when someone searches a data subject's name in a search engine (the "right to be forgotten"[75]), to exercises of the right to data portability,[76] and to their right to object to the processing of their data,[77] among other things. While the longer-term effects of the regulation remain to be seen, the regulation has already had an impact on the way the practices of data collection and processing are performed, both at the technological and the institutional levels, and has given citizens, advocates, and data protection authorities new avenues to contest data processing activities.[78]

In addition to changes in data processing activities and judicial challenges, the GDPR also resulted in the use of technological tools to solve some of the problems of technology. The privacy problems the GDPR sought to address are supposed to be fixed through technical means, such as "Data protection by design and by default",[79] embedding GDPR's normative

---

71 *D. Lee*, Tech Firms Struggle with GDPR Privacy Rules, 24.5.2018, <https://www.bbc.com> (last visited 7.9.2019); *A. Hern/J. Waterson*, Sites Block Users, Shut Down Activities and Flood Inboxes as GDPR Rules Loom, The Guardian, 24.5.2018, <https://www.theguardian.com> (last visited 28.9.2019).

72 *A. Bradford*, The Brussels Effect, Nw. U. L. Rev. 107 (2012), 1, 25.

73 *J. Brill*, Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data, MICROSOFT BLOG, 21.5.2018, <https://blogs.microsoft.com> (last visited 26.11.2019).

74 GDPR (note 22), Art. 15.

75 GDPR (note 22), Art. 17.

76 GDPR (note 22), Art. 20.

77 GDPR (note 22), Art. 21.

78 See Section III.

79 GDPR (note 22), Art. 25.

framework into the technology and the technology corporations' institutional practices.[80] The circularity of this type of solutionism does little to challenge or limit the business models that are driven by data analytics and which are perpetuating social and political problems.

More importantly, it delegated policymaking and decision-making regarding privacy rights – what they mean, who has them, how they are interpreted, where those rights extend jurisdictionally, etc. – to experts. On the one hand, legal experts and regulators framed, drafted, and ratified the regulations, and subsequently made judicial determinations as to their territorial reach and whether certain actions were in compliance with or violated the GDPR. Supervisory authorities and the European Data Protection Board have been delegated with ensuring compliance, enforcement, and the issuing guidelines and recommendations.[81] On the other hand, the GDPR granted technology corporations, lawyers, and engineers the power to make decisions as to how they would apply those regulations to their own companies and products relating to data processing. This is particularly the case in light of the GDPR's data protection by design provisions, which require that data protection and privacy protection be integrated into the technical infrastructure.[82] The GDPR effectively made people within technology corporations co-interpreters and co-constructors of what privacy means and how it gets operationalised.[83]

---

[80] This view is consistent with the idea that the same technologies that violate privacy can be used as a solution to that problem. *Floridi*, for example, argues that "digital ICTs are already providing some means to counterbalance the risks and challenges that they represent for privacy […] Digital ICTs do not necessarily erode privacy; they can also enhance and protect it." See *L. Floridi*, The Fourth Revolution: How the Infosphere is Reshaping Human Reality, 2014, 115.

[81] GDPR (note 22), Arts. 51-76.

[82] See *C. J. Hoofnagle/B. van der Sloot/F. Zuiderveen Borgesius* (note 31), 86; What Does Data Protection "by Design" and "by Default" Mean?, European Commission, <https://ec.europa.eu> (last visited 11.9.2020).

[83] On how engineers' vision of privacy gets operationalised and embedded in the technological products they create, see *A. E. Waldman*, Designing Without Privacy, Hous. L. Rev. 55 (2018), 659. On the role of coders and operators in designing technological devices which embed normative choices, see *F. De Vanna*, The Construction of a Normative Framework for Technology-Driven Innovations: A Legal Theory Perspective, in: E. Carpanelli/N. Lazzerini (note 28), 185 et seq.

2. The Discursive and Epistemological Shift

The GDPR's implementation was also accompanied by broader social changes, such as other jurisdictions adopting regulations which resemble or adopt its principles. The GDPR has come to attain a status as a model legislation to be aspired to or adopted in other jurisdictions. This had the effect of reconfiguring how a variety of institutions, cultures, and subjects consider the issues surrounding collection and processing of personal data.

Indeed, the GDPR has stabilised the public discourse around personal data collection practices as an issue of individual privacy. This can be seen in regulations modelled on the GDPR that are adopted elsewhere,[84] and institutional and corporate discourses that increasingly highlight privacy concerns,[85] centring discourse and knowledge of the problems associated with data collection on that issue. One prime example of this occurred in March 2019 when *Mark Zuckerberg*, the Chief Executive Officer (CEO) of Facebook, announced a redesign of the social media platform as part of a shift to privacy.[86] In that case, however, the shift to privacy meant a shift toward more private encrypted messaging between users on the platform. It also meant reduced permanence, interoperability, and secure data storage.[87] *Zuckerberg* interpreting what privacy is and should mean for users of his social media platform was based on, according to him, "what people really want".[88] By what means he determined that and what modes of deliberation

[84] *G. Greenleaf*, Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25.5.2018, University of New South Wales Law Research Paper No. 18-56, 3, (24.5.2018), <https://papers.ssrn.com> (last visited 26.11.2019); but see *A. Chander/M. E. Kaminski/W. McGeveran* (note 1). There are exceptions to this, of course, notably in the United States. *Chander*, *Kaminski*, and *McGeveran* argue that the California Consumer Privacy Act (CCPA) is an exception to this narrative which largely focuses on nation-states rather than the actors within them. While they argue that the CCPA was not modeled on the GDPR, they recognise that the CCPA and GDPR "herald a possible paradigm shift for data privacy" and that the GDPR functions subtly as a "privacy catalyst" even in the United States. See *A. Chander/M. E. Kaminski/W. McGeveran* (note 1), 24 et seq., 27.

[85] See, *e.g.* Report of the Special Rapporteur on the right to privacy, UN A/73/45712, 17.10.2018); *E. Schulze* (note 1); *E. Schulze*, Mark Zuckerberg Says He Wants Stricter European-Style Privacy Laws – But Some Experts Are Questioning His Motives, CNBC, 1.4.2019, <https://www.cnbc.com> (last visited 19.5.2019); *T. Cook*, It's Time for Action on Privacy, Says Apple's CEO Tim Cook, Time, 2019, <https://time.com/> (last visited 28.9.2019).

[86] *M. Zuckerberg*, A Privacy-Focused Vision for Social Networking, Facebook (2019), <https://www.facebook.com> (last visited 28.9.2019).

[87] *M. Zuckerberg* (note 86).

[88] *M. Zuckerberg* (note 86).

are implied in that statement are not clear. Moreover, *Srinivasan* has shown that Facebook's prior uses of the privacy discourse were instrumentalised as a means to drive out competitors.[89] Thus, it is not clear to what extent the current privacy discourse is mere window dressing for the benefit of the company, and why people should accept *Zuckerberg's* or Facebook's interpretation of privacy, given how past instances of Facebook invoking user privacy had problematic consequences.

The privacy discourse in relation to tech companies preceded the GDPR.[90] Other developments such as the news of the Cambridge Analytica data breach[91] that broke a few months before the GDPR became effective may have also contributed to its prominence. Yet the implementation of the GDPR, its extraterritorial reach, and its framing as a new "global standard" further solidified it on a transnational level. Many developments preceding the GDPR had already motivated wide public debates around privacy, including the use of "dataveillance" by governments since 2001 in the aftermath of 9/11[92] as well as *Edward Snowden's* revelations in 2013 of the surveillance activities by the intelligence agencies of the United States and the United Kingdom. Those debates, however, were more directly linked to government surveillance.

Of course, government surveillance both depends on,[93] and is constrained by, "surveillance intermediaries" or the "large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance".[94] While the National Security Agency (NSA) revelations revealed strong links between industry and government in the sharing of information and intelligence across borders for security purposes, the privacy debate in light of the GDPR has become particularly prominent in relation to technology firms that have gained huge amounts of

---

89 *D. Srinivasan*, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, Berkeley Business Law Journal 16 (2019), 39.

90 While the Lisbon Treaty, the OECD Privacy Principles, and the DPD all emphasised the right of privacy in relation to personal data collection and preceded the GDPR, it seems that none of them had the impact on the technological, normative, and discursive levels as the GDPR did.

91 *C. Cadwalladr/E. Graham-Harrison*, Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach, The Guardian, 17.3.2018, <https://www.theguardian.com> (last visited 7.9.2019).

92 *T. N. Cooke*, Cookies, in: M. B. Salter (ed.), Making Things International 2: Catalysts and Reactions, 2016, 228 et seq.

93 *B. E. Harcourt*, Exposed: Desire and Disobedience in the Digital Age, 2015, 79.

94 *A. Z. Rozenshtein*, Surveillance Intermediaries, Stanford L. Rev. 70 (2018), 99, 105.

economic and political power through the collection of massive amounts of personal data on their users. These massive datasets have created new market ecosystems around data collection, processing, aggregation, and analytics.[95] With the GDPR and other social shifts described here, the privacy discourse has become the dominant one in relation to technology corporations.

Thus, the GDPR also had an impact on knowledge and sense-making, marking a shift in how the problems associated with data collection and processing are collectively framed in its aftermath. This discursive and epistemological shift is accompanied by the exportation of European norms and values elsewhere,[96] as the GDPR reflects European values toward fundamental rights, including the rights to privacy and data protection.[97] *Christopher Kuner* has argued, for example, that given the GDPR's expressly extraterritorial reach, the EU is trying to promote its legal values as universal values.[98] The EU is currently recognised as a global privacy regulator due to its "de facto unilateral" influence.[99] These values reflect a particular European cultural and historical context where rights to privacy have received an elevated status.

3. The Normative Shift

The GDPR privileging European values of privacy over competing claims reflects political choices. Arguments for global harmonisation elide important political and distributive questions about these choices. For example, one might ask what is at stake when individual privacy becomes the dominant form of discussing and regulating the problems associated with data collection and processing? In the process, what other claims and whose

[95] *R. Kitchin*, The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences, 2014.

[96] But see *J. Scott*, Extraterritoriality and Territorial Extension in EU Law, Am. J. Comp. L. 62 (2014), 87 et seq. *Scott* argues that the EU is not seeking to export its own values elsewhere but rather is trying to enforce international standards. *J. Scott* (note 96), 112. I disagree with that contention in the case of the GDPR, as argued throughout this article.

[97] The rights to privacy and data protection are formally recognised in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) and Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union. See also, Section III above.

[98] *C. Kuner*, The Internet and the Global Reach of EU Law, in: M. Cremona/J. Scott (eds.), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law, 2018, 112 et seq.

[99] *P. M. Schwartz*, Global Data Privacy Law: The EU Way, N. Y. U. L. Rev. 94 (2019), 771, 774.

values have been backgrounded? What are the effects of framing these concerns as individual privacy issues on the social and political order in different cultural contexts?

While the practices of collection of personal data, classification, and standardisation are not new,[100] they have been framed as problems of knowledge production, power, or governance of populations rather than as problems of privacy. Even today, the issue of collection and processing of personal data could be framed as a distributional question, such as who gets to partake in the value created by data processing?[101] Highlighting privacy, as *Fleur Johns* and *Daniel Joyce* have noted, might reinforce "a disposition that tends to champion the distributive *status quo* in the name of freedom".[102]

The distributional impacts of data processing can also be extended to collective social costs imposed on people other than the individual data subject whose data is collected and processed. Individual-based data protection regimes are unable to address these issues.[103] Companies not only track information and inferences about particular individuals, but much of the value derived from data processing comes from the correlations and inferences these companies are able to make based on aggregated data.[104] In this way, personal data of an individual provides companies with information about other people. The individual aspect of privacy in the GDPR fails to account for the relational qualities of data processing and the collective interests they touch upon, which might require political mobilisation to address them rather than technical or technocratic solutions.[105]

Different ways of conceptualising what data processing is and how it works can also affect how people think it should be governed and around

---

100 See, *e.g. M. Foucault*, "Governmentality," Lecture at the Collège de France, 1.2.1978, in: G. Burchell/C. Gordon/P. Miller (eds.), The Foucault Effect: Studies in Governmentality, 1991, 87 et seq.; *J. C. Scott*, Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed, 1998; *G. C. Bowker/S. Leigh Star*, Sorting Things Out: Classification and Its Consequences, revised ed. 2000; *B. Anderson*, Imagined Communities: Reflections on the Origin and Spread of Nationalism, revised ed. 2016; *S. Jasanoff*, Virtual, Visible, and Actionable: Data Assemblages and the Sightlines of Justice, Big Data & Society 4 (2017), 1 et seq.

101 *F. E. Johns* (note 9), 27 et seq.

102 *F. E. Johns/D. Joyce*, Beyond Privacy: Is Prevailing Debate Too Analog for a Digital Age?, Human Rights Defender 23 (2014), 24.

103 *P. Pałka* (note 30).

104 *R. Kitchin* (note 95); *F. Pasquale*, The Black Box Society: The Secret Algorithms That Control Money and Information, reprint ed. 2015.

105 *P. Pałka* (note 30). *See also*, *S. Viljoen*, Democratic Data: A Relational Theory for Data Governance (11.11.2020), available at <SSRN: https://ssrn.com/abstract=3727562> or <http://dx.doi.org/10.2139/ssrn.3727562>.

what issues they mobilise for change. If one looks at the material infrastructures underlying data processing such as data centres and data servers, for example, one might highlight the environmental implications of the high energy usage and carbon emissions attributable to them.[106] One might also look at the resource extraction and labour necessary to make the materials that go into those infrastructures.[107] These examples illustrate how each framing prioritises certain values over others and *vis-à-vis* what competing forces or claims they ought to be considered.

V. Critiques of the GDPR

1. The Limits of Individual Privacy

Aside from the argument that the notion of privacy itself is contested,[108] contextually contingent,[109] unstable and subject to multiple meanings,[110] there are several additional limitations to approaching the problems associated with data processing from the angle of individual privacy. One such limit is that the individual is only incidental to big data analytics, and therefore, the focus on individual interests does not fit within current models of data analytics. These analytics detect patterns of behaviour and preferences on the basis of group profiling. This is why some scholars have argued for "group privacy" as a new concept for framings of the ethical, social, and political problems associated with data processing to better account for the collective harms and interests at stake.[111] Yet, even with the notion of "group privacy", the focus on privacy still overlooks other interests and harms that come into play with data analytics.

---

[106] *E. Bietti/R. Vatanparast*, Data Waste, 61 Harv. Int'l L. J. Online (2020), available at: <https://harvardilj.org> (last visited 11.9.2020).

[107] *K. Crawford/V. Joler*, Anatomy of an AI System, <https://anatomyof.ai> (last visited 3.2.2020).

[108] *D. K. Mulligan/C. Koopman/N. Doty*, Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy, Philosophical Transactions of the Royal Society A 374 (2016), 118, <https://royalsocietypublishing.org> (last visited 30.5.2020).

[109] *H. Nissenbaum*, Privacy in Context: Technology, Policy, and the Integrity of Social Life, 2009.

[110] See *L. A. Bygrave* (note 46); *D. J. Solove*, A Taxonomy of Privacy, U. Pa. L. Rev. 154 (2006), 477; *D. J. Solove*, Understanding Privacy, 2008.

[111] See *L. Taylor/L. Floridi/B. van der Sloot* (eds.), Group Privacy: New Challenges of Data Technologies, 2017.

As *Przemysław Pałka* has argued, the focus on the liberal value of individual privacy overlooks other social costs imposed by data-driven analytics today, such as price discrimination, behavioural manipulation, and social exclusion.[112] These are just a few examples where individual privacy has little to do with the risks and costs imposed on society by data analytics using aggregated data, which enables data-driven technological tools such as algorithmic decision-making, machine-learning, and artificial intelligence.[113] None of these tools would necessarily need to use individually identifiable information to perform their functions – anonymised data could still provide the capability to infer information and detect patterns on preferences and behaviour based on groups of individuals.[114] This information in the aggregate is what corporations using data analytics to promote commercial activity are after.[115] The collective and interconnected aspect of data analytics, as well as its collective harms, together illustrate just some of the shortcomings of the GDPR's individual privacy approach.

Moreover, in discussing what is being overlooked when we highlight privacy issues, *Stephen Humphreys* argues that as privacy has become an

> "inevitable anchor for contemporary anxiety in conditions of data excess, the concept may lack both the terminological precision for sharp analysis and the mobilising force for collective response".[116]

Some alternative framings that might be more helpful than privacy, he suggests, are some of its component elements, such as conscience, space, intimacy, sexuality, subjectivity, and autonomy.[117] By reframing pervasive data collection into an issue of conscience, the relationship between knowledge and authority becomes more central, and one can ask broader questions such as

> "how do changing conditions of knowledge production and dissemination, and shifting loci of authoritative access to, and evaluation of, this data, together redefine what it means to be a 'private person'?"[118]

---

112 *P. Pałka* (note 30).
113 *P. Pałka* (note 30), 19 et seq.
114 *P. Pałka* (note 30).
115 *P. Pałka* (note 30); *R. Kitchin* (note 95); *F. Pasquale* (note 104).
116 *S. Humphreys*, Conscience in the Datasphere, Humanity: An International Journal of Human Rights, Humanitarianism, and Development 6 (2015), 361 et seq.
117 *S. Humphreys* (note 116), 362.
118 *S. Humphreys* (note 116), 362.

Similarly, one might ask whether the traditional divide between the private sphere and the public sphere that many theories of privacy depend upon continues to make sense in the datasphere.[119]

Finally, another limitation of the privacy frame is that it can actually serve the interests of informational capitalism rather than challenge it.[120] Focusing on privacy leaves unchallenged the business models underlying informational capitalism and driving ever-expanding data collection and commodification.[121]

The GDPR's prioritisation of individual privacy and data protection rights reflects a preference for technical approaches to data governance,[122] while disregarding the differential impacts of these approaches on people around the world. Indeed, the idea of a global standard assumes a uniformity of cultural, economic, and institutional environments around the world that rarely exists.

The framing of social problems around technology shows how projects of technological governance are inextricably tied up with, or co-produce,[123] technological, normative, epistemological, and institutional orders. The next section provides an alternative framework of analysis which looks at how the GDPR is constructing subjectivity of EU data subjects and non-EU data subjects in ways that depoliticises the people and the technologies involved in data processing, followed by a case study on India and locally situated framings of problems associated with data collection and processing.

2. Constructing Political Subjects as Data Subjects

The GDPR's hopeful claim that "The processing of personal data should be designed to serve mankind"[124] might indicate a cosmopolitan ideal underlying its aims. Attempts to make the GDPR a global standard might also reflect similar cosmopolitan aims. While serving mankind is an honourable aspiration, the construction of people as data subjects has significant political implications. By constructing people as data subjects, the GDPR simultaneously constructs them as depoliticised objects from which data can be

119 *S. Humphreys* (note 116), 362.
120 See *S. Coll* (note 13).
121 See *J. E. Cohen* (note 11).
122 *F. E. Johns/D. Joyce* (note 102).
123 *S. Jasanoff* (note 6).
124 GDPR (note 22), Recital 4.

derived, extracted, and appropriated by capital, while granting them liberal rights of privacy that do not go far enough to protect their dynamic subjectivities.

The term "data subject" is defined within the GDPR under the definition of "personal data", as follows:

> "'[P]ersonal data' means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[125]

As *Käll* argues, this construction of personal data as an object also constructs people considered EU data subjects as objects, through their entanglement with their personal data.[126]

The GDPR is at once granting EU data subjects custodianship and control over their data, as it simultaneously legitimates the processing of data which gives others custodianship and control over their data. While the right to be forgotten and the right to data portability grant EU data subjects limited controls over the uses of their data, the GDPR is at the same time taking away their ability to prevent the fixing of their personhood or identity by technological tools and corporations, thus implying a passivity or lack of agency. This fixing of identity gives people flattened subjectivities which go against a dynamic subjectivity upon which democracy depends.[127] Yet, the GDPR does not protect these dynamic subjectivities in the name of privacy. Instead it creates flattened ones of its own through its liberal individualist framework.

The construction of EU data subjects as objects entangled with personal data and as passive subjects of law and technology is also accompanied by a construction of non-EU data subjects. By delineating a boundary between EU and non-EU data subjects, it constructs non-EU data subjects as passive subjects of the (data) market. These subjects of the market are constituted through market demands for personal data. While some might argue this is a stronger argument for global standardisation of regulatory frameworks based on the GDPR, I instead argue here that those arguments elide broader

---

125 GDPR (note 22), Art. 4.

126 *J. Käll*, A Posthuman Data Subject? The Right to Be Forgotten and Beyond, GLJ 18 (2017), 1145, 1154.

127 *J. E. Cohen* (note 40).

questions regarding the social and ethical constructs that are presumed to be acceptable in these practices and who makes those decisions.

There is nothing natural about the commodification of personal data. As *Polanyi* described the processes by which land, labour, and money were commodified and turned into fictitious commodities,[128] *Zuboff* describes how behaviour has undergone a process of commodification, turning personal data into the fourth fictitious commodity.[129] As subjects of the market, non-EU data subjects are constructed as passive subjects of data markets, which are co-produced with law and data processing technologies.[130]

The GDPR framework reconstructs political subjects into data subjects, who are simultaneously passive objects from which to derive personal data and subjects with liberal rights of privacy. Yet, privacy rights do not go far enough to protect their dynamic subjectivity as democratic citizens. This reconstruction, whether for EU data subjects or non-EU data subjects, rests on a presumption of subjectivity without agency and without politics. It thereby depoliticises both the subjects it helps construct and the technologies it helps shape. In the process, technologists and regulators become the *de facto* norm and ethics experts that decide what privacy is and ought to mean for society. These assumptions and constructions, along with their disempowering effects, tend to be left unquestioned in proposals to improve privacy and data protection, whether through legal or technological means.

The GDPR's reconstructions of subjectivity in depoliticising ways can be countered through local democratic engagement and deliberation. The next section will discuss recent engagements with a new proposed bill on data protection in India as one example of bringing democratic politics, agency, and local context back into the picture.

VI. Case Study: India

The GDPR has important distributive effects due to its impact and limitations on cross-border trade in data, having asymmetric effects on different

[128] *K. Polanyi*, The Great Transformation: The Political and Economic Origins of Our Time, 1944.

[129] *S. Zuboff*, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 2020.

[130] On law and legal privileges as constitutive of the construction of data markets, see *J. E. Cohen*, The Biopolitical Public Domain, in: J. E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism, 2019.

groups and countries.[131] These distributive effects are often overlooked when the discourse and framing of problems associated with data processing and analytics are framed as issues of individual privacy, and in arguments for creating global standards based on the GDPR.[132]

The GDPR regulates not only privacy, but also markets that trade in, or depend on, data.[133] In developing countries operating in the digital economy, such as India, the political and socio-economic context reflects a different set of values and concerns than those of the EU. In 2018, India developed a draft bill on personal data protection[134] (Bill) containing some principles modelled on the GDPR.

On the one hand, India has an incentive to comply with GDPR and provide "adequate protection" for data transfers from the EU in order to continue its software and data-related trade with the EU – a large contributor to its economic activity. On the other hand, its status as a developing country means that adopting privacy standards akin to those of the EU might limit the country economically, requiring a balancing between protecting privacy rights and its economic implications.[135]

Reflecting these concerns, the most recent version of the Bill currently before the Indian Parliament emphasises[136] the importance of boosting India's digital economy and the critical role of data in that economy.[137] Civil society groups such as the Centre for Communication Governance at National Law University Delhi, however, have taken issue with any prioritisation of economic growth at the cost of citizens' privacy. They argue that rooting the Bill in an "undefined idea of a digital economy" means prioritising the digital economy over individuals' rights.[138] This illustrates some of

131 *H. Lee-Makiyama*, The Political Economy of Data: EU Privacy Regulation and the International Redistribution of Its Costs, in: L. Floridi (ed.), Protection of Information and the Right to Privacy - A New Equilibrium?, 2014.

132 Some of these distributive effects have been discussed in Section IV. 3.

133 *H. Lee-Makiyama* (note 131), 86 et seq.

134 The Personal Data Protection Bill (2018), <https://meity.gov.in> (last visited 29.11.2019).

135 *A. Mattoo/J. P. Meltzer*, International Data Flows and Privacy: The Conflict and Its Resolution, JIEL 21 (2018), 769 et seq.

136 As of the time of writing this article.

137 The Personal Data Protection Bill, Bill No. 373 (2019), <https://www.prsindia.org> (last visited 11.9.2020).

138 Centre for Communication Governance at National Law University Delhi, Comments on the Draft Data Protection Bill, 2018 4, <https://ccgdelhi.org> (last visited 12.2.2020).

the concerns unique to the Indian context, which the GDPR framework overlooks.

In discussions prior to the release of prior versions of the draft Bill, the Indian Ministry of Electronics and Information Technology (MeitY) formed a committee to draft a bill on data protection and privacy. This Committee of Experts on a Data Protection Framework for India (Committee) released a white paper in November 2017, soliciting public comment and outlining key principles according to which the Committee felt should be prioritised in an Indian data protection bill. The Committee noted that the objective with a data protection bill for India is to "ensure growth of the digital economy while keeping personal data of citizens secure and protected".[139] The Committee also opened the debate to stakeholders to submit comments and held consultations in major cities, including Delhi, Mumbai, Bangalore, and Hyderabad.[140] In parallel to the Committee's efforts, advocacy movements like #SaveOurPrivacy developed their own draft model law called the Indian Privacy Code, 2018 and sought public comments.[141] This community effort built on some of the key principles the Committee outlined to try to protect Indian citizens' privacy rights in a way that took into account local understandings of the problems associated with data processing, including concerns about government surveillance and the digital economy. Moreover, with the unique technologies and histories in the Indian context, such as the biometric identity program Aadhaar, which is required for citizens to access government assistance, and India's history with the Sedition Law Act of 1870 and colonialism, mean that local concerns are vastly different from those reflected in the EU's GDPR.[142]

Collective knowledge claims about the social problems associated with science and technology vary according to civic epistemologies or "culturally specific, historically and politically grounded, public knowledge-ways", which can shape how those problems are addressed in different culturally situated contexts.[143] The Indian context shows the limits of copy-pasting

139 White Paper of the Committee of Experts on a Data Protection Framework for India, (2017).

140 Stake Holder consultation on Data Protection Framework, PRESS Information Bureau, Government of India, Ministry of Electronics & IT (2017), <https://pib.gov.in> (last visited 28.11.2019).

141 Internet Freedom Foundation, 7 principles of the Indian Privacy Code, Save Our Privacy (2019), <https://saveourprivacy.in> (last visited 28.11.2019).

142 *P. Arora* (note 12), 719.

143 *S. Jasanoff*, Designs on Nature: Science and Democracy in Europe and the United States, 2005, 249.

the EU's GDPR framework, as local understandings of the social problems associated with data processing and modes of deliberation differ from those in the EU. Nevertheless, it is clear that the influence of the GDPR can be seen in some of the provisions of the Bill, such as rights of correction, rights to data portability, and adequate protection for international data transfers, among other areas.

VII. Conclusion

Framing the GDPR as a global standard elides its political and cultural specificities. Globalisation of the GDPR ensures that a certain vision of the social good wins out over others through the expert language of law. Indeed, the EU's political and economic power and recognised expertise in regulating privacy issues have a great deal to do with why the GDPR's vision and its extraterritorial reach have actually had such a strong impact elsewhere.

Both data processing and its governance raise a number of political and normative questions which require sustained and deep democratic engagement, as well as avenues for diverse publics to imagine and decide their own visions of the social good. While the GDPR has been a well-intentioned effort to grapple with some of the problems of the data economy, and has provided ordinary citizens some useful mechanisms to directly challenge the practices of data collectors and processors, the exportation of the EU's regulatory framework and principles to other jurisdictions as a global standard does little to engage with deeper political questions or to reflect on its broader social effects. Rather, it reflects an attempt at universalisation of a particular technical fix to the political problems of informational capitalism.