13. Digital persona and transnational regulation of cyberspace

Nina Teresa Kiderlin and Shirin Barol

INTRODUCTION

Privacy regulation is a critical component of sustainable development as it ensures that the digital transformation respects human rights, fosters equity, and promotes responsible resource use. By mandating efficient data management practices and curbing superfluous data proliferation, privacy regulation inherently aligns technological ecosystems with environmental sustainability imperatives, thereby mitigating resource overuse. Simultaneously, such frameworks engender resilient economic growth by cultivating trust in digital infrastructures, safeguarding equitable competition, and fostering a climate of ethical innovation that supports diverse and inclusive markets. There has been rising concern over data protection of individual users interacting with cyberspace. Making money out of personal data is now a crucial part of the business model of technology companies all over the world. As users embrace online products and services offered by private sector entities, ensuring sustainable privacy regulation is a key concern. The public sector relies on its regulatory capacity to enforce private data protection of users. The following examples illustrate how privacy regulation is a new transnational concern triggering confrontation among the states.

The debate over banning TikTok reflects geopolitical tensions in the digital age. With over 170 million US users, TikTok's Chinese ownership raises concerns over data security and censorship. To address this, TikTok launched "Project Texas", storing US user data on Oracle servers. In 2024, the US Senate voted to force ByteDance to divest TikTok by 2025 or face a ban. TikTok argues this violates free speech, while critics question whether the ban serves national security or US competitors. Similarly, the EU's GDPR enforcement has challenged Meta's data practices. A 2024 ruling confirmed that Meta's broad data collection for targeted ads violated GDPR's data minimisation rules. This decision forces Meta and similar companies to restructure their data strategies, ensuring compliance with privacy regulations.

In both examples, market expansion, for example TikTok having US-based users, results in the private entity getting involved with a new set of regulatory constraints. For public authorities the legal mechanism has been a historical approach to enforce order and exercise control. Deploying this usual approach requires the jurisdictional boundary of public authority to match the operational jurisdiction of the private. However, global technology companies challenge the jurisdictional authority of nation states by creating new boundaries in the digital realm. The reimagination of boundaries challenges the traditional legal mechanisms of public authorities by limiting their power to exercise control.

This chapter analyses the consequences of new jurisdictional boundaries set by practices of private global technological companies. We argue that the legal boundary-setting practices of global technology companies follow what social scientists since the mid-twentieth century have identified as transnational. In these studies, the rising power of the private sector

challenged and surpassed the jurisdictional control demarcated by nation states. For instance, transnational corporations, for example BP or Siemens, leveraged the promise of a globalised market to set up production plants in many locations worldwide and have extensive reach and influence in multiple localities. The new operational scale of transnational corporations, particularly focused on production and trade at the time, resulted in private entities becoming critical actors of the global political economy. Scholars have captured this transformation by focusing on the changing dynamics of the relationship between private and public and how they constrain each other (Huntington, 1973).

As we demonstrate, transnational analysis is not limited to economic actors but it is also prominent in the social and political fields such as health and migration. While the return to geopolitics foregrounds confrontation among nation states as central to international affairs, the transnational turn is a reminder that other actors are also imposing challenges to the authority of nation states, as demonstrated through the cases of Facebook/Meta and TikTok above. In this chapter we ask what kind of geopolitical challenge the technology companies pose in the contemporary world. How is this geopolitical challenge interpreted in regulation? Who is the new regulatory subject?

To answer these questions, we first review how transnational has been approached in social sciences to demonstrate that global technology companies follow a historical pattern. The chapter discusses how monetisation of personal data is the profit-making strategy employed by these companies, informing broader privacy concerns. We analyse web tracking technologies, such as cookies, from law and technology perspectives as well as how monetisation of personal data of individual users by private sector companies leads to individualised regimes of data protection. We discuss how public regulation attempts to navigate the tension between domestic regulatory privacy concerns and transnational personal data flows. This tension is particularly visible between the European Union (EU) and non-EU states due to stricter regional regulation through, for example, the General Data Protection Regulation (GDPR). We argue that this new turn is framed as a geopolitical concern through concepts such as digital sovereignty. Digital sovereignty requires privacy regulations to protect individuals' data and ensure they retain control over personal information, promoting inclusivity and equity. Individuals interacting in cyberspace complicates the determination of which jurisdiction applies to them, for example by using a virtual private network (VPN). Therefore, transnational cooperation among nation states and private sector companies is necessary to achieve sustainability in this field. However, as we demonstrate in this chapter, the current geopolitical landscape is torn between protection of individual privacy and pervasive oversight and control over personal data. Considering this conflict, we argue that the digital persona as a new regulatory subject can assist geopolitical cooperation in the twenty-first century.

TRANSNATIONAL ANALYSIS IN SOCIAL SCIENCES

The current turn toward the analysis of the transnational in social sciences, for example in gender and migration scholarship, is complementary to the long-standing tradition of studies focusing on globalisation. While globalisation scholarship focuses on the global flows and more recently considers different sources of strains (Farrell and Newman, 2019), scholars of the transnational aspect complicate this view of the world by highlighting the opposition between domestic order and global flow. The proliferation of scholarship on the transnational

however, requires us to historicise the idea and see how during the last century the establishment of nation states as the provider of global order was encountered by the private attempt to surpass it. This tension might have been best captured in analysis of transnational corporations' involvement with newly independent states of the Global South during the second half of the twentieth century, which also marks the beginning of a new turn in geopolitical analysis (Cowen and Smith, 2009). Today, social scientists approach transnational processes by moving beyond the private entities and focusing on how non-state actors are involved with cross-border issues such as migration and public health. Overall, the emergence of this stream of research in the twentieth century partly allowed for a broader shift to take place in social sciences, which aims to surpass methodological nationalism (Burawoy, 2005; Mallard et al., 2024).

Since the mid-twentieth century, methodological nationalism has been identified as a problem in social sciences, calling for broader understanding of the global dynamics at play. This line of analysis critiques the extensive focus on nation states as a primary unit of analysis. Burawoy (2005) argues that this leads to a neglecting of transnational processes and global interdependencies in mainstream social sciences. The hybridity in studying transnational dynamics at play worldwide has opened the empirical horizon for different disciplines whilst simultaneously creating other challenges such as difficulties identifying scales of involvement for different actors in a single case. In the absence of the historical order steered by nation states, a fragmentation inherent to the field of transnational studies arises which requires critical collective reflection to determine the emerging power play. A historical overview of transnational analysis in social sciences provides a background upon which this reflection can be built when highlighting the geopolitical tension raised by private sector technology companies.

In an edited volume, published in 1971, Joseph Nye and Robert Keohane define "transnational relations" as interactions across state boundaries that are not necessarily part of the foreign policy domain. For these scholars, transnational interaction describes the "movement of tangible or intangible items across state boundaries when at least one actor is not an agent of a government or an intergovernmental organisation" (Nye and Keohane, 1971). For Samuel Huntington (1973), operating in between and with disregard of boundaries was not unprecedented, since armies and navies, churches and joint stock companies have all been similar, but the emerging transnational landscape of the 1970s was different in size, intensity and proliferation. He further argues that the terminological ambiguity between international, transnational and multinational inhibits scholars from capturing the consequent change in political economy. His attempt to distinguish between these terms allows him to argue that transnational operations have been developed out of the US national interest led by the international organisations in which Americans played a leading role. The expansion of transnational corporations requires access to different markets rather than acquisition, which was the prior mode of colonial expansion. Associating the rise of transnational organisation with the US expansion after the Second World War, he further argues the technological requirement to operate across jurisdiction can best function in the context of political collaboration (Huntington, 1973).

During the 1970s the rise of transnational corporations and their power in the global economy made scholars examine their impact on the state dynamic. Transnational corporations became a focus of analysis in the 1970s; they had expanded since the end of the Second World War and the simultaneous moment of increased independence. Scholarly attention to

transnational corporations was mostly focused on the possible sources of tension and kinds of influence this new type of corporation can have over the recently independent countries. The post-World War II transnational expansion of US-based companies, *inter alia* driven by economic reconstruction, technology transfer, and Cold War strategic alignment, was criticised by scholars and politicians. They raised questions about how US-based transnational corporations would influence the future of technological growth and relations between different domestic governments (Skully, 1976). The global entanglement of states and transnational corporations since the 1970s has informed analysis in which the main focus is to demonstrate that the confrontations between these entities define the new global order. On one hand the constraining power of the state, particularly in the countries of the Global South, was alarming, since the independence movement gradually provided the new states the capacity to practise sovereignty. However, the power of the modern production system offered by the standardisation allowed the transnational corporations to be a determining factor in the global market. The transnational corporations since the end of World War II have entangled the state in networks of interdependence. "For most dependency writers transnational corporations have constrained the exercise of state power by reinforcing transnational class alliances that link domestic compradores directly to the centres of international capitalism" (Biersteker, 1980). A decade later and in response to the rise of the transnational power of corporations, researchers started arguing that the countermovement of state resurgence is an impeding factor constraining the power of corporations through either adaptation of similar nationalist policies or the possibility to negotiate competitively with corporations.

Although political science and international relations as a discipline privileges a superiority over transnational analysis of global political economy, legal scholars might have had a more rigorous contribution in its conceptualisation due to law's attention to jurisdiction. In legal scholarship, the move toward the transnational allowed law to be analysed in a non-comparative way and to focus on the discursive construction of the entanglement between forms of ordering. Since the 1950s legal scholarship followed Phillip Jessup's (1956) call to theorise about a stateless legal regime through which the engagement of domestic and international law could be reimagined. In response, legal scholars have developed the concept of transnational law to discuss transboundary issues as they challenge our traditional understanding of politics and regulation (Jessup, 1956; Zumbansen, 2021). New forms of global interdependence question the legal understanding of jurisdiction as equality among sovereigns (Krisch, 2022). Legal studies have provided the transnational with a more structured framework in which it either addresses topics beyond nation states or legal orders imported and exported between borders (Shaffer, 2012). Using case studies, for example from bankruptcy, patent law, and anti-money laundry law from different countries, Shaffer measures the transnational as a factor against the state change.

The global technology companies leveraging cyberspace to offer services and products enforce a political change similar to the one sketched out here. While scholarship since the mid-twentieth century emphasised industrial production and trade as the primary vehicles for transnational actors to effect global change, the emerging dynamics of the digital turn demand a renewed focus. Global technology companies offer a key case study in understanding this shift. As personal data becomes a crucial resource for these companies, their access to diverse markets raises immediate privacy concerns for public authorities. How did technology companies end up monetising users' personal data? What are the socio-legal interpretations and broader implications of these practices?

CYBERSPACE, TRACKING MECHANISMS AND TRANSNATIONAL PRIVACY

In the early 2000s, the dotcom bubble burst served as a critical point of transformation for global technology companies. Demonstrating the potential for long-term profitability became a key struggle for companies offering internet-based services. To attract shareholders, web based companies needed to find ways to commodify and assetise online interactions, turning them into ongoing revenue streams. The solution, creating standardised units of digital measurement from everyday life data through quantification of activities and codification of human interaction, massively changed the twenty-first-century global technological landscape (Fourcade and Healy, 2024). This process of standardisation, intertwined with cyberspace's growing role in everyday life, has led to significant social and legal changes.

One of the earliest examinations of the precursor to this standardisation came from Oscar Gandy in 1993. Moving beyond states as the main subject of surveillance analysis, Gandy presented historical instances of how "corporate data machines" classified, clustered and segmented individuals into groups. His work highlighted the growing role of private entities in collecting and categorising personal data. More recently, social science has focused on contemporary capitalism's shift toward technoscientific capitalism (Mirowski, 2011) or the assetisation of technoscience (Birch and Muniesa, 2020).

Technoscience for them refers to the entanglement of scientific knowledge and technological practices, emphasising how they mutually shape each other. The term highlights the ways in which science and technology are co-produced, developed and applied in sociocultural, political and economic contexts. For example, the development of GPS technology illustrates this co-production. It is based on complex scientific principles such as relativity and advanced mathematics for calculating positions on earth from satellite signals. Military needs and geopolitical events during the Cold War influenced its development and expansion. Widespread civilian use of GPS transformed daily social life regarding transportation, emergency services, logistics, and social behaviour. Scholars analysing this co-production show how the turn toward financialisation and reliance on private capital since the 1990s forces a broader transformation in the field of science and technology to follow the logic and laws of the market. Shoshana Zuboff (2019) captures this shift through the concept of "behavioural surplus", where human data becomes a source of capital, driving the market toward "surveillance capitalism". This concept highlights how the extraction and analysis of personal data have become central to the contemporary economy. This market requires logged digital traces of human interaction within virtual spaces to be stored and repurposed for advertising. The numerisation and prediction of human behaviour created a new frontier for methodological advancements in data science, where the content and manner of every bodily and sensory interaction became a potential source for scientific endeavour. This transformation resulted in an intricate web of tracking technologies designed to monitor users and their behaviours.

Advancements in tracking technologies over the last decade have led to a new field of analysis, primarily populated by computer scientists focusing on studying privacy issues. Their studies focus on analysing these new technologies, and in particular engage with methodological challenges of uncovering the implications of tracking mechanisms as they emerge. One key outcome has been the analysis of cookie and fingerprinting-based tracking mechanisms. These studies emphasise how new mechanisms, such as flash cookies (Soltani et al.,

2010), Canvas Fingerprinting, and Evercookies (Acar et al., 2014; Englehardt et al., 2015), are designed to circumvent users' knowledge and attempts to delete cookies. For computer scientists, a crucial element is the methodological capability to capture and analyse these developments.

While web tracking is partly enabled by developments in big data storage and analysis, it also stems from the financial transformation of technology companies. Since the 2008 financial recession, the regulatory shift toward managing risk in the investment industry has resulted in new capital streams flowing into technology. Similar to arguments made by scholars of technoscientific capitalism, increased investment in technological development across different fronts over the last decade has contributed to the fragmentation of solutions and services in this field. For example, numerous start-ups and companies in the 2010s became involved in processing online payments across different jurisdictions, promising to create efficiency and security. Although fragmentation is a common feature in the process of change within any classificatory system or organisation, the consequent restructuring of tracking mechanisms has made web navigation a vulnerability for users' privacy. For social scientists, the process of turning technological solutions into financial opportunities by tracking people's everyday behaviour supports the digital advertising industry's use of algorithms (Hwang, 2020) and makes measuring and analysing personal data a natural outcome (Ruckenstein and Schüll, 2017). The promise of seamless personalisation is the core competitive advantage offered by private sector companies to consumers, whose personal data, aggregated through surveillance mechanisms, embeds automation into the decision-making process.

Legal scholars, approaching privacy from a regulatory perspective, have highlighted the legal developments that shape the possibility of surveillance. For Cohen (2019a), the legal system is not merely a superstructure overseeing technological development but actively contributes to how these developments unfold. Critiquing studies that portray law and technology as under-regulated, Cohen (2019b) introduces the concept of "legal entrepreneurship" to capture how regulatory frameworks actively constitute normal economic behaviour in this market. Through this legal lens, the technical analysis of privacy is supplemented by an understanding of how surveillance rationality structures cyberspace. Furthermore, the contingency of informational capitalism and law has emphasised the need to redraw the contours between public and private entities. Informational capitalism is an economic system where the production, accumulation and exchange of information and data are central to generating value, shaping industries, and driving social and technological dynamics. For example, Pasquale (2015) discusses how the privatised control of algorithms reconfigures public accountability and inclusion due to automated decision-making. Similarly, Benkler (2019) addresses rising inequality resulting from the new power gained by skill-based technical change in different societies.

Beyond the changing power of the private sector, the crucial role of cyberspace in everyday life in the twenty-first century has led scholars to examine necessary legal adaptations. They grapple with methodological and conceptual requirements for reimagining law in the age of cyberspace. Addressing the problem of how private power in informational capitalism tends to be insulated from democratic control, legal scholars seek options for accountability. For instance, Rahman (2017) draws on public utility and private control arguments to discuss how to impose control over access to different infrastructural goods, including online platforms. For Kapczynski (2019), the insulation of the market through the extensive use of trade secrecy law requires critical examination and reconfiguration to allow for democratic oversight. Responses to this concern range from arguments that no new regulatory approach

is needed for cyberspace (Easterbrook, 1996) to those advocating a complete reimagining of legal practice and enforcement (Johnson and Post, 1996). This spectrum demonstrates the diverse possibilities for addressing the intersection of law and cyberspace.

As legal scholars experiment with situating technology within a broader constellation, the definition of jurisdiction emerges as a key factor. Scholars of cyberspace law who have designed new regulatory models with respect to the emerging definition of jurisdiction in cyberspace argue that data flows are not restricted by jurisdictional boundaries. Consequently, the legal challenge is to understand how legal institutions and structures must evolve to adapt. Empirically, private sector companies offering services in cyberspace rely on different methods to determine individual user jurisdiction. These varied methods present an intriguing case study of how territorial affiliations are negotiated between users and providers, driven by a mix of legal and business necessities. Beyond proof of residential address, the most traditional way to determine jurisdiction and widely used in legacy banking services, new approaches rely on phone number area codes or IP addresses.

Although providers primarily base their choice of method on trade regulations and research conducted on individual markets, the only option left for users is to participate in individualised regimes of cyber interaction. While individualisation allows access to personal schemes customised by the needs and preferences, privacy protection is now also a personal concern. Consequently, legal scholars have begun to explore the possibility of reimagining cyberlaw beyond the jurisdictional control of the state, focusing on individual user digital personhood.

The concept of a "digital persona" argues that a holistic view of a user's entangled life in cyberspace is possible if we move beyond an instrumentalist view of technology and adopt a substantivist approach (Pasquale and Cockfield, 2018). The latter allows scholars to take a reactionary role in designing legal mechanisms to protect individual users whose online interactions do not necessarily follow physical constraints. As we discuss in the next section, the individualisation of regimes of privacy informs a broader turn among users modifying boundaries in cyberspace. The digital persona, as described by Pasquale and Cockfield, is shaped by external forces such as law and technology. They argue that this integration increasingly determines how individuals are treated in both the digital and physical worlds, leading to the need for stronger legal protections against manipulation, discrimination, and data misuse. Their framework suggests that digital personhood should not just be about controlling what third parties know but about proactively protecting autonomy in the online world.

DOMESTIC PRIVACY REGULATION AND TRANSNATIONAL DATA FLOWS

The twenty-first century is characterised by a rapidly increasing transnational flow of personal data due to technological advancement coupled with market liberalisation. Relying on services provided through the internet challenges data flow and privacy regulation as those are by and large domestic, intended to be applied within the physical territory of a nation state. Cross-border data flows necessitate that this issue moves to the international realm, creating challenges for development and enforcement of regulatory frameworks (LeSieur, 2012). Nation states are therefore in a challenging position; they on the one hand have to support cross-border commerce, which automatically contains transnational data flow, and on the other hand strive to protect the data privacy of their citizens. This tension between domestic

privacy concerns and regulation is particularly visible when data flows to jurisdictions that have significantly different privacy protection levels than the data origin country, exemplified earlier in this chapter through the GDPR case. Regulators which are based in the more restrictive jurisdiction can react to this by aiming to limit transnational data flow, often citing customer protection and privacy concerns which cannot be granted (Mattoo & Meltzer, 2018).

Global companies place a great emphasis on free data flow to facilitate seamless global trade. This increases pressure for regulators to develop common or interoperable data protection regulation frameworks that do not impede international exchange of goods and services, which rely on seamless data flow (Mattoo & Meltzer, 2018). Cross-border data flow is a crucial element in the spread of technology/knowledge, enabling for example financial services and online shopping/retail across international borders.

Historically, data protection has been a domestic issue and therefore international harmonisation of regulation regarding cross-border personal data flows online is difficult. Rules overlap, standards are not compliant with each other, and nation states have divergent historical positions on the regulation of personal data: the United States often defer to state-level legislation, the EU harmonised their regulation regionally through GDPR for example, whilst China and Russia aim to regulate data locally (Voss, 2019; Farrell & Newman, 2019), creating competing standards (Drezner, 2005).

Shaffer (2000) points out that conflicts over privacy regulation are not solely international but also take place within nation states depending on their form of federal governance in which often EU regulation changes the power balance between different non-EU domestic interest groups. US regulators end up promoting data privacy self-regulation by businesses to avoid open conflict with the EU and often US businesses to indeed implement EU standards in data privacy measures in what Shaffer describes as "transnational regulatory conflict and interdependence" (Shaffer, 2000). Similarly, the "Brussels effect" describes how EU regulation impacts non-EU domestic regulation and businesses (Bradford, 2020). Non-EU actors adopt some EU regulation or sign agreements such as the Safe Harbour Framework for cross-border data flows to avoid lawsuits in EU courts.

The European Union frames data flow and privacy concerns under the umbrella term "digital sovereignty" (Giddens, 2020), a policy alternative to surveillance capitalism and techno-authoritarianism. It can be understood as an attempt to (re-)claim authority in cyberspace, following earlier attempts by states to transpose legal instruments applicable in the interconnected but analogue world to the digital (Pohle & Thiel, 2020; Jenerette et al., 2006). Digital sovereignty is an attempt by nation states to establish themselves in a central governing position in cyberspace, irrespective of how cross-border data flows, online communication, and the exchange of goods and services seem to operate in a space not necessarily covered by domestic jurisdictions. Digital sovereignty is the capacity of states, organisations or individuals to exert control over digital infrastructure, data governance, and technological autonomy, ensuring independence from external influence while safeguarding rights and security in cyberspace.

Multiple pieces of domestic and regional legislation govern the transnational personal data from one region (EU) to other countries (Voss, 2019), often improving the privacy of constituents whilst simultaneously complicating the process due to compliance issues. Regulation design and enforcement is further complicated by the storage and data outsourcing to third parties (Gunasekara, 2009), as well as different policy priorities and cultural understandings of "privacy" as either a right of the individual or as an impediment to efficient internet usage.

Whilst the EU is more focused on the rights of individuals, the US prioritises a business-friendly environment with few grievance mechanisms for individuals, and China favours a national interest approach to data flow regulation and subsequently there is very limited regulatory harmonisation on a state level (Voss, 2019; De Hert & Papakonstantinou, 2016). Currently, the data sovereignty and privacy agenda reflects this fragmentation as it ranges from tolerating co-existence of different interpretations, regulations and policies, to attempts of establishing the hegemony of one regional or domestic regulatory regime (Adler-Nissen & Eggeling, 2024). States arguing for digital sovereignty (ranging from the EU to China and the US) have created mechanisms by which their citizens expect the state to protect their personal data online, be it for security reasons, enforcement of cultural norms, or to combat disinformation (Pohle & Thiel, 2020).

However, day-to-day interactions of individuals with cross-border companies in cyberspace are characterised in a multitude of ways by users evading digital sovereignty restrictions. Different solutions such as Virtual Private Networks (VPNs) provide users with the choice of different domestic jurisdictions. A VPN works by encrypting an individual user's internet traffic and routing it through a secure server in a location of their choice, allowing them to mask their IP address, protect their privacy, and access content as if they were in the selected jurisdiction.

Legal scholars are increasingly interested in understanding the implications of jurisdiction-hopping practices on domestic and international regulation (Mishra, 2021). This use of VPNs reinforces the importance of the digital persona as a regulatory subject following the transnational practices of technology companies. Whilst users are moving beyond different jurisdictions, the regulators are working to determine the type of control they are able to exercise. The users' reliance on VPNs can be taken as a sign that they understand it as a tool of access as well as privacy protection, following the general trend toward quantification of self. However, considering the pervasive tracking as well as ever-increasing volume of personal data, the regulators need to re-think the approach towards jurisdiction and subject. Highlighting the geopolitical nature of developing an interoperable regulatory framework requires a holistic view towards digital personhood as a subject of regulation.

CONCLUSION

The interplay between privacy regulation, sustainability and geopolitics underscores the complex dynamics shaping the governance of global digital ecosystems. As transnational corporations increasingly leverage personal data as a key economic resource, they simultaneously challenge traditional regulatory frameworks and national jurisdictions. These developments bring into sharp relief the necessity of sustainable approaches to privacy regulation that balance individual rights, innovation, and geopolitical stability.

Sustainability in this context extends beyond environmental concerns to include economic resilience, social equity, and ethical data practices. Privacy regulations play a pivotal role in fostering a sustainable digital economy by ensuring that personal data is managed responsibly and equitably. Such frameworks not only protect individuals from exploitation but also promote trust in digital systems, a cornerstone for long-term technological and economic progress. Fransisco and Heintz discuss related challenges of digital governance with a particular focus on artificial intelligence in Chapter 14 of this volume. They observe a turn towards soft law in

governance of artificial intelligence, exacerbating inherent global inequalities. Furthermore, sustainability necessitates efficient data governance to mitigate resource-intensive practices such as unnecessary data storage and processing, aligning digital transformation with broader environmental goals.

Geopolitically, privacy regulation represents a critical frontier where national interests, economic power and technological sovereignty converge. The rise of global technology companies has blurred the lines between domestic and international regulatory domains, creating friction among states and between public authorities and private sector entities. This tension is particularly evident in debates over digital sovereignty, where governments seek to assert control over data flows while maintaining the openness essential for global commerce. These geopolitical considerations often reflect deeper ideological divides, as states prioritise differing values such as individual privacy, national security or economic growth.

To reconcile these competing imperatives, it is essential to foster transnational cooperation and harmonised regulatory frameworks. This involves not only aligning privacy standards but also addressing power asymmetries between states and corporations. The concept of a "digital persona" offers a pathway to bridge these divides, providing a user-centric lens that respects individual autonomy while accommodating the transnational nature of data flows. Such an approach highlights the shared responsibility of states and corporations in creating a fair and inclusive digital ecosystem.

Ultimately, sustainable privacy regulation should navigate the intricate intersections of geopolitics, technological innovation and global interdependence. By prioritising equity, transparency and collaboration, policymakers can craft governance models that uphold human rights, foster economic stability, and ensure that digital transformation contributes positively to sustainable development on a global scale.

REFERENCES

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014, November). The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 674–89).

Adler-Nissen, R., & Eggeling, K.A. (2024). The discursive struggle for digital sovereignty: Security, economy rights and the Cloud Project Gaia-X. *JCMS: Journal of Common Market Studies, 62*(4), 993–1011.

Benkler, Y. (2019). Don't let industry write the rules for AI. *Nature*, *569*(7754), 161–2.

Biersteker, T.J. (1980). The illusion of state power: Transnational corporations and the neutralization of host-country legislation. *Journal of Peace Research*, *17*(3), 207–21.

Birch, K., & Muniesa, F. (Eds.). (2020). *Assetization: Turning Things Into Assets in Technoscientific Capitalism*. MIT press.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Burawoy, M. (2005). Response: Public sociology: populist fad or path to renewal?. *British Journal of Sociology*, *56*(3).

Cohen, J.E. (2019a). *Between Truth and Power*. Oxford University Press.

Cohen, J.E. (2019b). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *Surveillance & Society*, *17*(1/2), 240–45.

Cowen, D., & Smith, N. (2009). After geopolitics? From the geopolitical social to geoeconomics. *Antipode*, *41*(1), 22–48.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review*, *32*(2), 179–94.
Drezner, D.W. (2005). Globalization, harmonization, and competition: The different pathways to policy convergence. *Journal of European Public Policy*, *12*(5), 841–59.
Easterbrook, F.H. (1996). Cyberspace and the law of the horse. *University of Chicago Legal Forum*, 207.
Englehardt, S., Reisman, D., Eubank, C., Zimmerman, P., Mayer, J., Narayanan, A., & Felten, E. W. (2015). Cookies that give you away: The surveillance implications of web tracking. In *Proceedings of the 24th International Conference on World Wide Web*, 289–99.
Farrell, H., & Newman, A.L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79.
Fourcade, M., & Healy, K. (2024). *The Ordinal Society*. Harvard University Press.
Gandy, O.H. (2021). *The Panoptic Sort: A Political Economy of Personal Information*. Oxford University Press.
Giddens, A. (2020). "Foreword". In C. Hobbs (ed.), *Europe's Digital Sovereignty*. London: ECFR. Available from: https://ecfr.eu/archive/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf.
Gunasekara, G. (2009). The "final" privacy frontier? Regulating trans-border data flows. *International Journal of Law and Information Technology*, *17*(2), 147–79.
Huntington, S.P. (1973). Transnational organizations in world politics. *World Politics*, *25*(3), 334–68.
Hwang, T. (2020). *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*. FSG originals.
Jenerette, G.D., Wu, W., Goldsmith, S., Marussich, W.A., & Roach, W.J. (2006). Contrasting water footprints of cities in China and the United States. *Ecological Economics*, *57*(3), 346–58.
Jessup, P. (1956). *Transnational Law*. Yale University Press.
Johnson, D.R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367–402.
Kapczynski, A. (2019). The law of informational capitalism. *The Yale Law Journal*, *129*(5), 1460.
Krisch, N. (2022). Jurisdiction unbound: (Extra) territorial regulation as global governance. *European Journal of International Law*, *33*(2), 481–514.
LeSieur, F. (2012). Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy. *International Data Privacy Law*, *2*(2), 93.
Mallard, G., Barol, S., & Kiderlin, N.T. (2024). The United States in the world today: How sociologists think about it and why it matters. *Annual Review of Sociology*, 50.
Mattoo, A., & Meltzer, J.P. (2018). International data flows and privacy. *Journal of International Economic Law*, *21*, 769–89.
Mirowski, P. (2011). *Science-mart: Privatizing American Science*. Harvard University Press.
Mishra, N. (2021). Breaking down digital walls: The interface of international trade law and online content regulation through the lens of the Chinese VPN measure. *Brooklyn Journal of International Law*, *47*, 359.
Nye Jr, J.S., & Keohane, R.O. (1971). Transnational relations and world politics: An introduction. *International Organization*, *25*(3), 329–49.
Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information*. Harvard University Press.
Pasquale, F., & Cockfield, A. J. (2018). Beyond instrumentalism: A substantivist perspective on law, technology, and the digital persona. *Mich. St. L. Rev.*, 821.
Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4).
Rahman, K.S. (2017). The new utilities: Private power, social infrastructure, and the revival of the public utility concept. *Cardozo Law Review*, *39*, 1621.
Ruckenstein, M., & Schüll, N.D. (2017). The datafication of health. *Annual Review of Anthropology*, *46*(1), 261–78.
Shaffer, G. (2000). Globalization and social protection: The impact of EU and international rules in the ratcheting up of US privacy standards. *Yale Journal of International Law*, *25*(1).
Shaffer, G. (2012). Transnational legal process and state change. *Law & Social Inquiry*, *37*(2), 229–64.

Skully, M.T. (1976). The transnational corporation: A critical analysis of its prospects. *The Australian Quarterly*, *48*(3), 73–82.
Soltani, A., Canty, S., Mayo, Q., Thomas, L., & Hoofnagle, C.J. (2010, March). Flash cookies and privacy. In *2010 AAAI Spring Symposium Series.*
Voss, W.G. (2019). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*(3), 485.
Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *PublicAffairs, New York*.
Zumbansen, P.C. (2021). 'Transnational law: Theories & applications' in P.C. Zumbansen (ed.) *The Oxford Handbook of Transnational Law*, Oxford University Press.