INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Geopolitics, jurisdiction and surveillance

Monique Mann
Department of Criminology, Deakin University, Geelong , Australia, monique.mann@deakin.edu.au

Angela Daly
Law School, University of Strathclyde, Glasgow, United Kingdom, a.daly@strath.ac.uk

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1501

Abstract: The rise of digital information communication technology has major implications for how states wield coercive power beyond their territorial borders through the extraterritorial geographies of data flows. In examining the geopolitics of data, transnational surveillance, and jurisdiction, this collection makes a significant contribution to the field of global internet governance. It shows how the internet is a forum for geopolitical struggle with states weaponising jurisdiction and exerting power beyond their own borders directly, and via infrastructures owned and operated by transnational technology companies. These dynamics challenge existing conceptual and theoretical categories of contemporary law across the fields of international relations, criminology, and digital media, and raise urgent questions about if and how individual rights can be protected in an era of ubiquitous transnational surveillance conducted by private companies and governments alike.

Keywords: Surveillance, Power, Jurisdiction

Article information

Published: 16 Sep 2020

Funding: Mann received funding as part of her Vice-Chancellor's Research Fellowship in Technology and Regulation, and from the Intellectual Property and Innovation Law (IPIL) Programme, at Queensland University of Technology. This supported the original workshop, copy-editing and editorial assistance.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/geopolitics-jurisdiction-surveillance

Citation: Mann, M. & Daly, A. (2020). Geopolitics, jurisdiction and surveillance. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1501

PAPERS IN THIS SPECIAL ISSUE

GEOPOLITICS, JURISDICTION AND SURVEILLANCE

INTRODUCTION

With this special issue we offer critical commentary and analysis of the geopolitics of data, transnational surveillance and jurisdiction, and reflect upon the question of if and how individual rights can be protected in an era of ubiquitous transnational surveillance conducted by private companies and governments alike. The internet provides a number of challenges, and opportunities, for exercising power, and regulating, extraterritorially to the sovereign nation

state. These practices are shaped and influenced by geopolitical relations between states. Certainly, the trans-jurisdictional nature of the internet means that the legal geographies of the contemporary digital world require rethinking, especially in light of calls for a more sophisticated and nuanced approach to understanding sovereignty to govern, and also protecting individual rights in the electronic age (Johnson & Post, 1996; Goldsmith & Wu, 2006; Brenner, 2009; Hilderbrandt, 2013; Svantesson, 2013; 2014; 2017; DeNardis, 2014). These issues raise a host of additional contemporary and historical questions about attempts by the US to exert power over extraterritorial conduct in various fields including crime, intellectual property, surveillance and national security (see e.g., Bauman et al., 2014; Boister, 2015; Schiller, 2011). Yet dynamics are shifting with the emergence of the new technological superpower China, and regulatory efforts of the European Union (for example via the General Data Protection Regulation). The emergence of large transnational corporations providing critical virtual and physical infrastructure adds private governance to this equation, which offers further new dimensions to the rule of law and also self- or co-regulation (see for example Goldsmith & Wu, 2006; DeNardis & Hackl, 2015; Brown & Marsden, 2013; Daly, 2016).

The idea for this special issue emerged from a workshop that we co-convened in 2016 in which we sought to explore a range of questions: the impact of domestic and international cybercrime, data protection and intellectual property laws on sovereignty and extraterritoriality; the geopolitical impacts of domestic and international surveillance and cybercrime laws such as the Council of Europe's Convention on Cybercrime (Budapest Convention), the recent United States Clarifying Lawful Overseas Use of Data (CLOUD) Act and other lawful access regimes including European Union e-Evidence proposals; the application of due process requirements in the contemporary policing of digital spaces; the objectives of justice in the study of private governance in online environments; and the implications of these transnational developments for current and future policy and regulation of online activities and spaces.

Since 2016, we have witnessed striking developments in the geopolitical and geoeconomic relationships between states, global technology companies, their transnational surveillance practices, and corresponding governance frameworks. In particular, the rise of China and the globalisation of its internet industry is a major development in this time, along with the Trump presidency in the US and the ensuing trade war (Daly, in press). Just in the weeks prior to the publication of this special issue, there was significant escalation of tensions between the US and China played out via the restriction of social media companies' access to the US market. On 6 August 2020, Donald Trump issued executive orders banning transactions with ByteDance (Tik Tok's parent company) and Tencent (WeChat's parent company) that are subject to US jurisdiction, stating that "the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States ". Surveillance and sharing US citizens' data with the Chinese Communist Party, protection of intellectual property from corporate espionage, and Chinese censorship and disinformation were cited as justification supporting the purge. Subsequently, Trump issued a further executive order requiring that ByteDance sell off all of TikTok's US based assets. These types of geopolitical struggles are examined further in Cartwright's timely contribution to this special issue on '*Internationalising state power through the internet*' (Cartwright, 2020).

Further to the recent US-Chinese tensions, in the month prior to publication of this collection, the Court of Justice of the EU (CJEU) handed down its landmark decision in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (" *Schrems II*") (2020) invalidating the EU-US Privacy Shield (following *Schrems I* invalidating the predecessor EU-US

Safe Harbour agreement in 2015) with significant ramifications for the transfer of the data of EU citizens to the US as a consequence of the US' extensive state surveillance, and insufficient safeguards protecting privacy. The exact impacts that this decision will have for transborder data transfers are yet to be fully understood, but will undoubtedly be significant. At the same time, the US is negotiating executive agreements under its Clarifying Lawful Overseas Use of Data (CLOUD) Act that allow for authorised states to access the content of communications held by US technology companies without prior judicial authorisation, *and* for the US to compel US technology companies to provide access to data stored extraterritorially to the US jurisdiction (as per the initial *Microsoft* case rendered moot by the introduction of the CLOUD Act, see further Warren, 2015; Svantesson, 2017; Mann & Warren, 2018; Mulligan, 2018).

This all comes at a time when nations, and indeed regions, are asserting their "digital sovereignty" through data localisation initiatives that limit transborder data flows, as witnessed recently with France and Germany enacting their plans for European digital sovereignty (ANSSI, n.d.) and the corresponding launch of the GAIA-X cloud computing project (GAIA-X, n.d.) that creates a European data infrastructure independent of both China and the US.

China has also started asserting itself legally beyond its territorial borders. Hong Kong's new controversial National Security Law includes provisions which criminalise secession, subversion, terrorism, and collusion with foreign powers and via Art 38, purports to apply to non-HK permanent residents committing these offences even if they are based in other countries. In addition, Art 43 enables the Hong Kong Police Force when investigating national security crimes to direct service providers to remove content and provide other assistance. How these provisions will be applied to Hong Kong's transnational internet (which to date has included both Chinese and Western internet companies and services including some which are banned in mainland China) remains unclear, some US-based companies such as Facebook and Twitter have already announced their suspension of compliance with data requests from the Hong Kong authorities (Liao, 2020).

Taken together, these most recent developments highlight the significance of the geopolitical and geoeconomic dimensions of data, private-public surveillance interests, and associated impacts for human rights and international trade. They also demonstrate that extraterritoriality is no longer just a feature of US internet law and policy and equally that national sovereignty is no longer just a feature of Chinese internet law and policy.

These dimensions become more relevant with the concurrent reinforcement of physical borders amid a new global crisis brought by the COVID-19 pandemic that also has significant implications for cross-border information sharing and data storage e.g., immunity passports, contact tracing applications with data stored on the cloud (see Taylor et al., 2020). Certainly, expanded surveillance and information collection by states and private companies have proven to be central to the global response to bio(in)security created by the pandemic, with significant extraterritorial implications (Privacy International, 2020). For example, one of the main criticisms leveled at the Australian COVIDSafe contact tracing application was that Amazon was contracted to host the contact tracing information on its web services (AWS), with the potential for the US to access the data via the US technology company. In response, and like Germany and France, the Australian government is considering the development of a "sovereign cloud" for the storage of Australia's data (Besser & Welch, 2020; Sadler, 2020). Nevertheless, the pandemic response has also demonstrated the transnational corporate power of Google and Apple as key gatekeepers to the operation of government-backed COVID contact tracking apps, despite the questionable or unproven effectiveness of these apps in automating contact tracing (Braithwaite

et al., 2020). Google and Apple have even become the source of apps that offer improved data protection when compared to the in-house attempts of various European governments to create their own apps (Daly, in press), yet simultaneously cement their infrastructural power (Veale, 2020).

MAIN CONTRIBUTIONS TO THIS SPECIAL ISSUE

With these brief introductory remarks in mind, we turn to the overview of the papers and their main contributions to this issue. We open the collection with Oskar J. Gstrein's contribution *'Mapping power and jurisdiction on the internet through the lens of government-led surveillance'* (Gstrein, 2020) that examines governance frameworks for the regulation of government-driven surveillance to avoid the 'balkanisation' of the internet. Two proposals are analysed, namely, the 'Working Draft Legal Instrument on Government-led Surveillance and Privacy', presented to the United Nations Human Rights Council, and the proposal for a 'Digital Geneva Convention' (DGC) by Microsoft's Brad Smith. The article questions whether it is possible to create an internet based on human rights principles and values. Interlinked with issues of human rights online, our own (along with Adam Molnar) contribution on *'Regulatory arbitrage and transnational surveillance'* (Mann, Daly, & Molnar, 2020) examines developments regarding encryption law and policy within 'Five Eyes' (FVEY) countries, specifically the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth 1) in Australia. We argue that this new law is significant both domestically and internationally given its extraterritorial reach enables the development of new ways for Australian law enforcement and security agencies to access encrypted telecommunications via transnational providers, and allows for Australian authorities to assist foreign counterparts in both enforcing and potentially circumventing their domestic laws. We show that deficiencies in Australian human rights protections are the 'weak link' in the FVEY alliance, which means there is the possibility for regulatory arbitrage to exploit these new surveillance powers to undermine encryption, at a global scale, via Australia.

Madison Cartwright's article *'Internationalising state power through the internet: Google, Huawei and geopolitical struggle'* (Cartwright, 2020) shows how the US has exploited the international market dominance of US-based internet companies to internationalise its own state power through surveillance programmes. Using Huawei as a case study, Cartwright also examines how Chinese companies threaten the dominance of US companies as well as the geopolitical power of the US state, and in response, how the US has sought to shrink the 'geo-economic space' available to Huawei by using its firms, such as Google, to disrupt Huawei's supply chains. The analysis demonstrates how states may use internet companies to exercise power and authority beyond their borders. Extraterritorial exercise of power by non-state actors is explored further in *'Public and private just wars: distributed cyber deterrence based on Vitoria and Grotius*' (Thumfart, 2020). In Johannes Thumfart's contribution, the role of non-state actors in cyber attacks are considered from the perspective of just war theory. He argues that private and public cyber deterrence capacities form a system of distributed deterrence that is preferential to state-based deterrence alone.

In *'Going global: Comparing Chinese mobile applications' data and user privacy governance at home and abroad'* Lianrui Jia and Lotus Ruan argue that differential levels of privacy and data protection demonstrate the importance of jurisdictional influences in the regulatory environment and argue this shapes the global expansion of Chinese internet companies (Jia & Ruan, 2020). They examine the governance of Chinese mobile applications at a global scale and

their comparative analysis of international-facing versions of Chinese mobile apps versus Chinese-facing versions demonstrates greater levels of data protection are proffered to those users located outside China than those within. Continuing with the theme of transnational data protection, in *'Transnational collective actions for cross-border data protection violations'* Federica Casarosa examines alternative forms of enforcement, specifically, transnational collective actions in the European Union as an avenue to empower data subjects and achieve remedies for data protection infringements (Casarosa, 2020). Casarosa uses the Cambridge Analytica-Facebook scandal to highlight the multijurisdictional and cross-border nature of data protection violations, examines some of the limits of existing redress mechanisms under the EU's General Data Protection Regulation (GDPR), and argues for greater scope for transnational collective actions where associations or non-government organisations represent claimants from various jurisdictions.

Cross-border access to data is a central concern for transnational online policing. In the contribution on *'The legal geographies of extradition and sovereign power'* Sally Kennedy and Ian Warren raise a series of questions about access, use and exchange of digital evidence under mutual legal assistance treaty (MLAT) requirements (Kennedy & Warren, 2020). Via a case study concerning a Canadian citizen facing extradition to the US, they show how US sovereignty and criminal enforcement powers are advanced with implications for global online criminal investigations. Their analysis shows a need for clearer transnational data exchange protocols or the possibility of shifting prosecution forums to the source of online harm, arguing that this would promote fairness for those accused of online crimes with a cross-jurisdictional aspect. Matters of e-evidence are further explored in '*Anchoring the need to revise cross-border access to e-evidence'* in which Sergie Vazquez Maymir examines the European Commission's e-evidence package, including the 'Proposal for a Regulation on European Production and Preservation Orders' and associated impact assessment. He critically analyses the arguments and evidence supporting the EPO regulation and the policy shift away from Mutual Legal Assistance to direct cooperation. Vazquez Maymir argues that the problems associated with cross border access to e-evidence are framed in terms of technical and efficiency considerations, and in doing so, the political and economic motivations are lost.

CONCLUSION

Utilising, and in some cases exploiting, information communication technology to exert private and public power across multiple jurisdictions undoubtedly creates new challenges for traditional forms of regulatory governance and the protection of human rights. Each of the papers in this collection raise and speak to critical questions about the type of internet that we want (free, open, unified and decentralised?), and the role that states and companies (should) play in creating it. The papers demonstrate the significance of the internet as a forum for geopolitical struggle and the weaponisation of jurisdiction, especially with exterritorial reach, for states to extend their power beyond their own borders directly, and via transnational companies.

While the US, due to historical reasons as the birthplace of the internet and the *de facto* international hegemon in the 1990s/2000s, has been the focus for private and public extensions of political and economic power via the internet, the increasing multipolarity of the world and its impact on technology law and policy is impacting upon the relationship between jurisdiction and power online, as can be seen through this collection's contributions. The EU has been gaining prominence as a 'regulatory superpower' especially since the introduction of the GDPR,

and the emergence of China as a global internet player is now also apparent through the globalisation of its internet services and the extraterritorial reach of the new Hong Kong National Security Law. Increasing attention ought to be paid to such developments beyond the US and EU, particularly from BRICS countries, and how these interact with, and impact upon, global internet governance and internet law and policy with the West too.

ACKNOWLEDGEMENTS

Mann received funding as part of her Vice-Chancellor's Research Fellowship in Technology and Regulation, and from the Intellectual Property and Innovation Law (IPIL) Programme, at Queensland University of Technology. This supported the original workshop, copy-editing and editorial assistance.

Angela Daly would like to thank University of Strathclyde Scholarly Publications and Research Data/Open Access@Strathclyde, and in particular Pablo de Castro, for making a financial contribution to support this special issue being made available on an open access basis. She would also like to thank the Queensland University of Technology IPIL Programme for financially supporting the original workshop.

We would like to thank Dr Kayleigh Murphy for her excellent editorial assistance. We would especially like to acknowledge and thank Frédéric Dubois and the entire *Internet Policy Review* team for their enthusiasm and support in publishing this collection. We thank the participants at the workshop we held at QUT in 2016, and the international peer-reviewers that contributed their expertise and constructive comments on the papers (including ones that did not make it into the final collection): Songyin Bo, Balázs Bodá, Evelien Brouwer, Lee Bygrave, Jonathan Clough, Robert Currie, Jake Goldenfein, Samuli Haataja, Blayne Haggart, Danielle Ireland-Piper, Tamir Israel, Martin Kretschmer, Joanna Kulesza, Robert Merkel, Adam Molnar, Gavin Robinson, Stephen Scheel, James Sheptycki, Nic Suzor, Dan Svantesson, Peter Swire, Johannes Thumfart, Natasha Tusikov and Janis Wong.

REFERENCES

A.N.S.S.I. (n.d.). *The European Digital Sovereignty—A Common Objective for France and Germany*. https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144. https://doi.org/10.1111/ips.12048

Besser, L., & Welch, D. (2020, April 23). Australia's coronavirus tracing app's data storage contract goes offshore to Amazon. *ABC News*. https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682

Boister, N. (2015). Further reflections on the concept of transnational criminal law. *Transnational Legal Theory*, *6*(1), 9–30. https://doi.org/10.1080/20414005.2015.1042232

Braithwaite, I., Callender, T., Bullock, M., & Aldridge, R. W. (2020). Automated and partly automated contact tracing: A systemic review to inform the control of COVID-19. *The Lancet Digital Health*. https://doi.org/10.1016/s2589-7500(20)30184-9

Brenner, S. W. (2009). *Cyber Threats: The emerging fault lines of the nation state*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195385014.001.0001

Brown, I., & Marsden, C. T. (2013). *Good governance and better regulation in the information age*. MIT Press.

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

Casarosa, F. (2020). Transnational collective actions for cross-border data protection violations. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1498

Daly, A. (In press). Neo-Liberal Business-As-Usual or Post-Surveillance Capitalism With European Characteristics? The EU's General Data Protection Regulation in a Multi-Polar Internet. In R. Hoyng & G. P. L. Chong (Eds.), *Communication Innovation and Infrastructure: A Critique of the New in a Multipolar World*. Michigan State University Press.

Daly, A. (2016). *Private Power, Online Information Flows and EU Law: Mind the Gap*. Hart.

Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (C□311/18), (The Court of Justice of the European Union (Grand Chamber) 2020). http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9745404

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press. https://doi.org/10.12987/yale/9780300181357.001.0001

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunication Policy*, *39*, 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

Executive Order on Addressing the Threat Posed by TikTok. (2020). The White House. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-

threat-posed-tiktok/

GAIA-X. (n.d.). *GAIA-X: A Federated Data Infrastructure for Europe*. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.

Gstrein, O. (2020). Mapping power and jurisdiction on the internet through the lens of government-led surveillance. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1497

Hildebrandt, M. (2013). Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace. *University of Toronto Law Journal*, *63*(2), 196–224. https://doi.org/10.3138/utlj.1119

Johnson, D., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Kennedy, S., & Warren, I. (2020). The legal geographies of extradition and sovereign power. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1496

Liao, R. (2020, July 8). The tech industry comes to grips with Hong Kong's national security law. *TechCrunch*. https://techcrunch.com/2020/07/08/hong-kong-national-security-law-impact-on-tech/

Mann, M., Daly, A., & Molnar, A. (2020). Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1499

Mann, M., & Warren, I. (2018). The digital and legal divide: Silk Road, transnational online policing and southern criminology. In K. Carrington, R. Hogg, J. Scott, & M. Sozzo (Eds.), *The Palgrave handbook of criminology and the global south* (pp. 245–260). Palgrave MacMillan. https://doi.org/10.1007/978-3-319-65021-0_13

Mulligan, S. P. (2018). *Cross-Border Data Sharing Under the CLOUD Act* (No. 7-5700 R45173; CRS Report). Congressional Research Service. https://fas.org/sgp/crs/misc/R45173.pdf

Order Regarding the Acquisition of Musical.ly by ByteDance Ltd. (2020). The White House. https://www.whitehouse.gov/presidential-actions/order-regarding-acquisition-musical-ly-bytedance-ltd/

Privacy International. (2020). *Tracking the Global Response to COVID-19*. https://privacyinternational.org/examples/tracking-global-response-covid-19

Sadler, D. (2020, July 7). Government Finally Backs Sovereign Cloud Capability. *Innovation Aus*. https://www.innovationaus.com/govt-finally-backs-sovereign-cloud-capability/

Schiller, D. (2011). Special commentary: Geopolitical-economic conflict and network infrastructures. *Chinese Journal of Communication*, *4*(1), 90–107. https://doi.org/10.1080/17544750.2011.544085

Svantesson, D. (2013). A 'layered approach' to the extraterritoriality of data privacy laws.

International Data Privacy Law, *3*(4), 278–286. https://doi.org/10.1093/idpl/ipt027

Svantesson, D. (2014). Sovereignty in international law – how the internet (maybe) changed everything, but not for long. *Masaryk University Journal of Law and Technology*, *8*(1), 137–155. https://journals.muni.cz/mujlt/article/view/2651

Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press. https://doi.org/10.1093/oso/9780198795674.001.0001

Taylor, L., Sharma, G., Martin, A., & Jameson, S. (Eds.). (2020). *Data Justice and COVID-19: Global Perspectives*. Meatspace Press. https://shop.meatspacepress.com/product/data-justice-and-covid-19-global-perspectives

Thumfart, J. (2020). Private and public just wars: Distributed cyber deterrence based on Vitoria and Grotius. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1500

Vazquez Maymir, S. (2020). Anchoring the Need to Revise Cross-Border Access to E-Evidence. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1495

Veale, M. (2020, July 1). Privacy is not the Problem with the Apple-Google Contact-Tracing Toolkit. *The Guardian*. https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights

Warren, I. (2015). Surveillance, criminal law and sovereignty. *Surveillance & Society*, *13*(2), 300–305. https://doi.org/10.24908/ss.v13i2.5679

FOOTNOTES

1. Cth stands for Commonwealth, which means “federal” legislation, as distinct from state-level legislation.