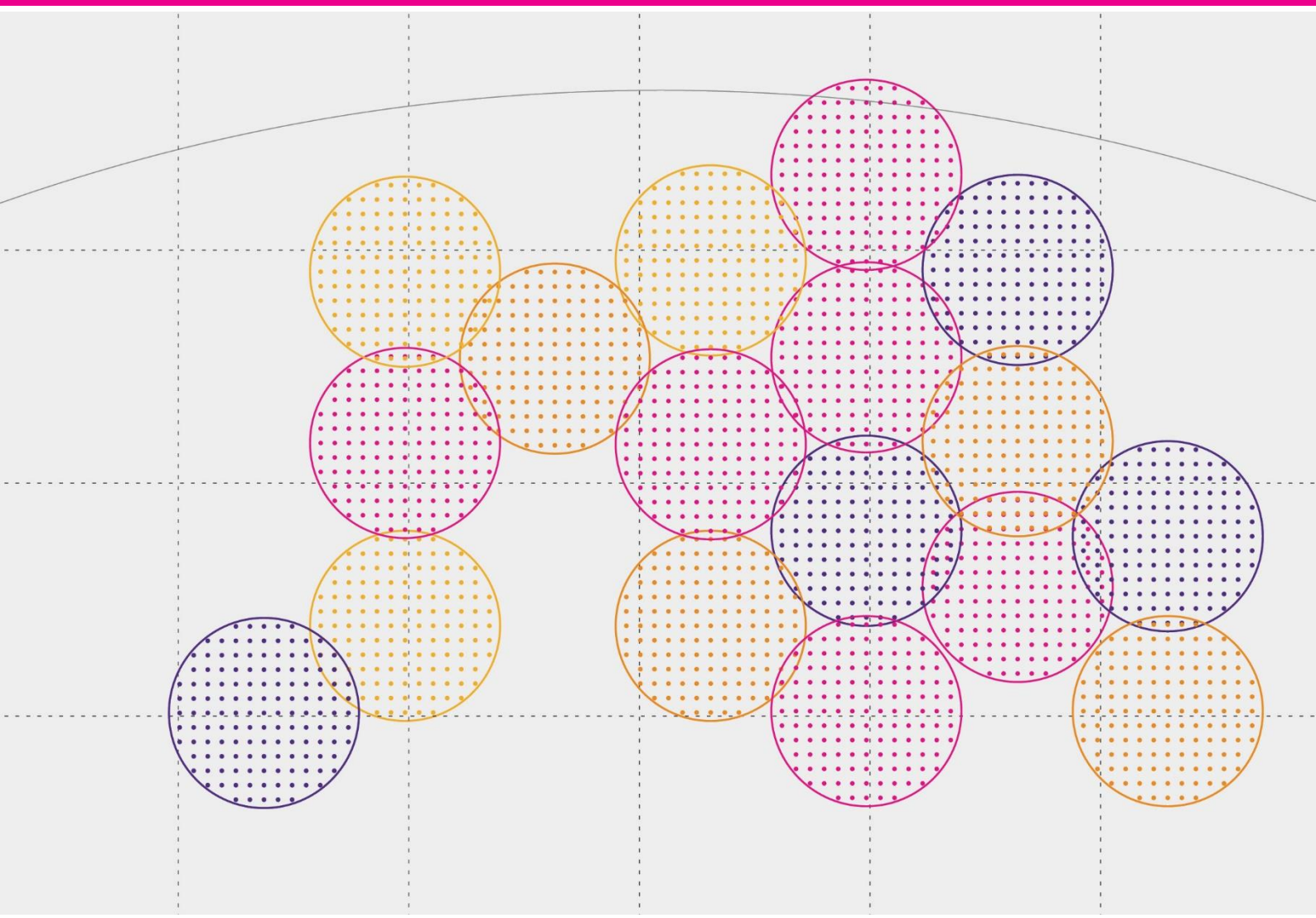
Digital Sovereignty: the overlap and conflict between states, enterprises and citizens

August 2020

Sam Wood, Stacie Hoffmann, Mark McFadden, Akhiljeet Kaur, Sarongrat Wongsaroj, Aude Schoentgen, Grant Forsyth, Laura Wilkinson



plumconsulting.co.uk

About Plum

Plum offers strategy, policy and regulatory advice on telecoms, spectrum, online and audio-visual media issues. We draw on economics and engineering, our knowledge of the sector and our clients' understanding and perspective to shape and respond to convergence.

About Oxford Information Labs

Oxford Information Labs (OXIL) is a cyber intelligence company founded in 2002 with roots in Internet policy and research. OXIL provides consultancy and bespoke technical solutions to clients across the world.

About this paper

This paper explores the differing interpretations of digital sovereignty among states, enterprises and citizens, and explores the implication of these differences for the future of the global internet.

Plum Consulting
10 Fitzroy Square
London
W1T 5HP

T +44 20 7047 1919
E info@plumconsulting.co.uk

Contents

Introduction

Although there is no universal definition, digital sovereignty[1] is an umbrella term that refers to the ability to exercise control over digital assets, such as data, content or digital infrastructure, or over the use of those assets. While this concept has arguably existed for decades, it has gained a new currency for a number of reasons, including concerns about state surveillance (stemming from the 2013 Snowden revelations), concerns over the level of dependence on extranational infrastructure and systems, concerns over online harms, and a desire to claim more of the economic benefits of cyberspace.

Nations across the globe have differing interpretations of digital sovereignty. China has created, in effect, a separate internet ecosystem, over which the state maintains an unparalleled degree of control. The US, on the other hand, is a staunch supporter of the open internet and the current "multistakeholder" model of internet governance. Between these two poles are a slew of other nations seeking to balance an interoperable, international internet with increased national agency over the internet.

These interpretations of digital sovereignty also affect other stakeholders: enterprises and citizens. Enterprises must navigate an increasingly diverse set of national regulations on data localisation, data protection, and online harms. They are also keen to maintain control over an exceptionally valuable asset – their data – as well as maintaining users' trust.

At the same time, citizens and civil society organisations are arguing for greater user control over how their personal data is obtained, stored used and removed (*personal* data sovereignty), pushing back against both enterprises and governments (who have incentives to collect ever greater amounts of user data). In some societies citizens can and are undertaking collective action to exercise digital sovereignty, and to push their governments to adopt more stringent data protection rules.

This paper reflects on the concept of digital sovereignty and how it is being interpreted around the world. It considers the international context of internet governance and how certain nations are acting to enhance or protect their digital sovereignty. It then considers how enterprises and civil society are acting to exert sovereignty over their own digital assets, most notably data. Finally, it reflects upon the implications of these developments for the global internet, and the future evolution of the concept.

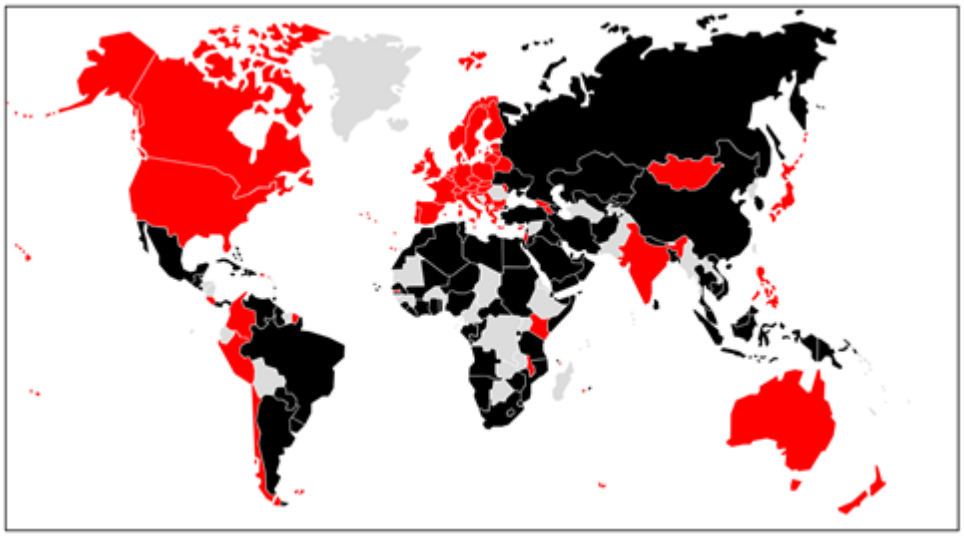
[1] Cyber sovereignty and internet sovereignty are terms used for a similar concept. A related concept is data sovereignty, which refers to the ownership, management and regulation of data, and is considered here to be part of the broader concept of digital sovereignty.

1 Digital sovereignty – the international context

The 2012 ITU World Conference on International Telecommunications (WCIT) highlighted the divergence in interpretations of digital sovereignty. A proposal from Russia, China, Saudi Arabia, Algeria and Sudan called for "equal rights" for all governments to manage internet numbering, naming, addressing and identification resources. This would have given governments a more central role in Internet governance, in contrast to the current "multistakeholder" approach (in which relevant stakeholders, including governments, the business sector, civil society and experts develop common rules and standards for operating the Internet).

Although this proposal was eventually shelved, a contentious vote was held on a non-binding resolution suggesting that the ITU should *"continue to take the necessary steps for ITU to play an active and constructive role in the development of broadband and the multi-stakeholder model of the internet."*[2] Eighty nine nations, largely non-Western countries, ultimately supported the proposal (see map).

Figure 1.1: Country positions on ITR proposed at WCIT 2012 (signatories in black)[3]



This is perhaps unsurprising. Many nations have a sense of being left out when it comes to decisions around internet governance.[4] The multistakeholder model is perceived as being dominated by Western interests, particularly the US.[5] This is increasingly being seen as an anachronism in an era where an increasing proportion of internet users are in the global south and east.[6] Moreover, many states – particularly developing nations – feel they do not have sufficient resources to fully participate in the current internet governance process.[7]

By contrast, stakeholders in favour of the multistakeholder model in the US and European nations were opposed to an extension of the scope of the International Telecommunications Regulations (ITR) Treaty to cover internet governance. They argued that the current approach has encouraged innovation and economic growth.[8] There

[2] BBC (2012). Available at: https://www.bbc.co.uk/news/technology-20717774 [Accessed July 2020]
[3] Masnick, M. (2015). Available at: https://www.techdirt.com/articles/20121214/14133321389/who-signed-itu-wcit-treaty-who-didnt.shtml [Accessed July 2020]
[4] Dutton, W. (2016). Multistakeholder Internet Governance? *World Development Report 2016 Digital Dividends*. http://pubdocs.worldbank.org/en/591571452529901419/WDR16-BP-Multistakeholder-Dutton.pdf
[5] Thimm, J. and Schaller, C. (2014). Internet Governance and the ITU: Maintaining the Multistakeholder Approach. Available at: https://www.cfr.org/report/internet-governance-and-itu-maintaining-multistakeholder-approach
[6] Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs 91: 1 (2015) 111–130.*
[7] Thimm, J. and Schaller, C. (2014).
[8] Lunden, I. (2012). Available at: https://techcrunch.com/2012/11/30/if-it-aint-broke-dont-fix-it-eu-adds-its-voice-to-the-chorus-opposing-more-internet-regulation-ahead-of-key-itu-dubai-meeting/ [Accessed July 2020]

are also concerns that an expanded role for governments in internet governance would embolden illiberal regimes to increase their control over cyberspace (for example, through censorship).[9]

While the practical impact of the resolution was limited, it highlighted the divergence in views on the relationship between national sovereignty and cyberspace.[10] At the time The Economist noted that "*…the world now splits into two camps when it comes to the internet: one is comprised of more authoritarian countries, which would like to turn back the clock and regain sovereignty over their own national bits of the internet; the other wants to keep the internet and its governance as it is*".[11]

Viewed from 2020, this black and white division appears somewhat simplistic. States are increasingly charting alternative paths which fall short of the degree of control asserted by Russia and China (see below) but nevertheless envisage a significant role for the state in the governance and management of cyberspace.[12] The Norwegian Institute for International Affairs noted that some European countries – Poland, Hungary and the UK – have introduced legislation enhancing governmental control over the internet. It noted *"the clear democracy–non-democracy divide might not be as applicable as it seemed just a few years ago"*.[13] Even supporters of the 'free' internet, such as France and Germany, are tempering that support with increased protections for users (like GDPR) and measures to support and protect their domestic tech sectors.[14]

A 2018 study by New America argues that countries can be grouped into three broad clusters in terms of internet governance: sovereign and closed, global and open and digital deciders – "*states that remain largely undecided and possess the capacity to influence the global conversation*".[15] The latter group includes countries like India and Brazil, which might decisively influence the trajectory of international processes. However, the authors noted a general drift of states toward the 'sovereign and closed' pole.

One reason for this shift towards greater level of government involvement is the emergence of new technologies, including artificial intelligence, machine learning and blockchain (see Section 3). This is born not only out of governments' desire to encourage economic growth, but also to ensure they have a strong voice in future governance and standard-setting debates. Other motivations include a desire to encourage the domestic tech sector, to ensure adequate protections for users' data, and to protect users from online harms. Illiberal regimes might also wish to extend their control over the internet in order to manage access to information and suppress dissent.

The consequence of this is a diversity of different approaches to tackling issues such as online harms, data protection and cross-border data flows. This is resulting in growing regulatory and technical fragmentation of the global internet. Enterprises must navigate a world of increasingly diverse national regulations, for example different user privacy initiatives (such as in Brazil and the EU). This may make it more challenging to do business across borders if it is not clear where and to whom data can be transferred.

This is particularly the case for the global tech giants, which own vast collections of user data stored across multiple jurisdictions. This can create conflicts when law enforcement in one country request access to data

[9] Thimm, J. and Schaller, C. (2014).
[10] Similar issues resurfaced at the 2014 ITU conference in Busan, Korea, this time without the contentious vote. See Dickinson, S. (2014). *How will internet governance change after the ITU conference?* Available at: https://www.theguardian.com/technology/2014/nov/07/how-will-internet-governance-change-after-the-itu-conference
[11] The Economist (2012). *A digital cold war?* Available at: https://www.economist.com/babbage/2012/12/14/a-digital-cold-war
[12] Sherman, J. (2019). *How Much Cyber Sovereignty is Too Much Cyber Sovereignty?* Available at: https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty
[13] Schia, N. and Gjesvik, L. (2017). Norwegian Institute for International Affairs (NUPI). Retrieved July 24, 2020, from www.jstor.org/stable/resrep07952
[14] Morozov, E. (2018). *Reasserting cyber sovereignty: how states are taking back control.* Available at: https://www.theguardian.com/technology/2018/oct/07/states-take-back-cyber-control-technological-sovereignty
[15] Morgus, R. et al (2018). *The Digital Deciders*. Available at: https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/two-poles-and-three-clusters

stored in another country – as observed when the US requested data from Microsoft that was stored in an Irish data centre.[16]

[16] Linklaters LLP (2019). *U.S. CLOUD Act and GDPR - Is the cloud still safe?* Available at: https://www.lexology.com/library/detail.aspx?g=72241f56-b87e-41d5-8a6e-150d09365a25

2 States and digital sovereignty

In this section we discuss how various states interpret the concept of digital sovereignty, and the measures being taken by certain states to enhance or protect their digital sovereignty.

The motivation of states to action is not always articulated or apparent. Some states, notably Russia and China, argue that national governments should be the ultimate arbiters of what happens in cyberspace, even at the cost of international interoperability. Others appear to be motivated more by economic concerns, such as the desire to ensure a leading position in emerging technologies. Data protection is also a recurring theme, as states attempt to both protect their citizens and to ensure a valuable asset (personal data) remains in-country.

The states analysed have been selected to reflect a wide range of views on the issue of digital sovereignty. They represent major or emerging players in the field of internet governance, and their stance is likely to shape the international debate around internet governance in the years to come.

2.1 Brazil

Brazil's focus in this area has largely been on promoting data sovereignty and data protection. It has instituted the *Lei Geral de Proteção de Dados*, (LGPD) or the General Data Protection Law 2020. The law has a wide scope and applies to both online and offline personal data across both private and public sectors. The objectives of the law are to guarantee individual rights and foster economic & technological innovation.[17]

Under the bill, individuals have a right to access their data, rectify it, cancel or exclude it, ask for an explanation and interoperability of data transfer. Similar to the EU's General Data Protection Regulation (GDPR) and the Indian Data Protection Bill 2019, Brazil's LGPD has extraterritorial application. Any company that collects and processes the data of people in Brazil, regardless of their nationality, comes under the purview of the law. The law is also applicable to any foreign company with an office in Brazil or any firm that offers services to Brazil's market. Some of the exemptions to the law are national and public security, pure research, and artistic and journalistic purposes.[18]

Individual consent is not the only permissible grounds for data processing - it is just one amongst ten legal bases[19] listed in the LGPD. At least one of these legal bases should be fulfilled while performing the data processing operation.[20] However, the lawful basis for the data processing purpose must be made clear to the individual by the data processing entity and should also be documented. The Brazilian government claims to take account of the interests of all the stakeholders including the data processing firms by having a broad list of legal bases for data processing. As per the government, this approach would stimulate innovation in Artificial Intelligence and Machine Learning ecosystems and foster economic growth for Brazil.[21] This provision is a departure from both the GDPR and the Indian Data Protection bill 2019, both of which hold individual consent as a pre-requisite for any data processing operation.

Like in India and Europe, Brazil's government has also considered measures for data localisation. The Central Bank of Brazil proposed a draft regulation - 'Cybersecurity Policies and the Procurement of Data Processing,

[17] Privacy Tracker (2018). The new Brazilian General Data Protection Law — a detailed analysis. Available at: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/
[18] Ibid.
[19] According to LGDP the legal bases for data processing are consent, compliance with a legal or regulatory obligation, execution of public policies, research, execution of a contract, exercising of rights in judicial, administrative, or arbitration procedures, protection of life or physical safety, protection of health, protection of legitimate interests, protection of credit. See: https://relentlessdataprivacy.com/understanding-the-data-protection-act-of-brazil-lgpd/
[20] Relentless Data Privacy (2020). Understanding the Data Protection Act of Brazil (LGPD). Available at: https://relentlessdataprivacy.com/understanding-the-data-protection-act-of-brazil-lgpd/
[21] Privacy Tracker (2018).

Data Storage, and Other Cloud Computing Services (57/2017)' - that would require local data storage for financial data.[22] However, that has not been implemented due to opposition from local and international software companies and businesses using cloud-computing services.

Prior to this a provision mandating data localisation was also added into Brazil's 'Internet Bill of Rights' that was passed in December 2014, in response to the Snowden revelations. However, the provision was eventually removed because of opposition from multiple fronts and was instead replaced with a clause asserting Brazilian jurisdiction over data and services offered in Brazil.[23]

2.2 China

China's assertion of sovereignty over its cyberspace can be dated back to the 1990s, when the internet was explicitly brought under state control.[24] Since then it has developed a sophisticated apparatus for oversight of its cyberspace. Through wide-ranging content-filtering and censorship (dubbed 'the Great Firewall') it has created, in effect, a separate internet ecosystem.[25] Far-reaching data localisation requirements,[26] restrictions on encryption,[27] deep packet inspection,[28] and indigenous technology requirements[29] give Chinese authorities unparalleled control of the national cyberspace.

Ideologically China sees digital sovereignty as the absolute right of the state to control its domestic internet environment, and the content citizens are exposed to.[30] Xi Jinping has argued that countries have the right to choose how to regulate their internet, and called upon countries *"to respect one another's cyber sovereignty*."[31] This, along with cybersecurity, is seen as vital for maintaining China's core values.[32]

This holistic notion of sovereignty includes physical infrastructure, data, and the Chinese internet's naming and addressing systems. The approach to sovereignty goes so far that China is actually proposing to standardise a new internet architecture in the International Telecommunication Union (ITU) which would use what China calls a 'new Internet protocol' to restructure these foundational elements of the internet in a way that reflects its approach to digital sovereignty and further separate internet ecosystems at the technical and governance layers.[33]

Despite its control of domestic cyberspace, China has taken steps to ensure the protection of personal information, such as the Cyber Security Law (in force from June 2017), which bans online service providers from

[22] BSA The Software Alliance (2017). Comments on the Brazilian Central Bank´s Proposed Regulation on Cybersecurity Policies and the Procurement of Data Processing, Data Storage, and Other Cloud Computing Services – Public Consultation 57/2017. Available at: https://www.bsa.org/files/policy-filings/11212017CommentsonCentralBankRegulations_English.pdf

[23] The Centre for Internet and Society (2019). The Localisation Gambit: Unpacking policy measures for Sovereign control of Data in India. Available at: https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

[24] At the time (1996), there were just 150,000 Chinese internet users. See: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190826_digital_authoritarianism_polyakova_meserole.pdf

[25] Xu, Y. (2016). Deconstructing the Great Firewall of China. Available at: https://blog.thousandeyes.com/deconstructing-great-firewall-china/

[26] Wei, Y. (2018). Chinese data localization law: Comprehensive but Ambiguous. Available at: https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/

[27] McKune, S. & Ahmed, S. (2018). The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda. *International Journal of Communication 12(2018), 3835–3855*

[28] Margolin, J. (2016). Russia, China, and the Push for "Digital Sovereignty. Available at: https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/

[29] Hoffmann, S., Bradshaw, S. & Taylor, E. (2019). Networks and Geopolitics: How great power rivalries infected 5G. Available at: https://oxil.uk/publications/geopolitics-of-5g/

[30] Schia, N. & Gjesvik, L. (2017). China's cyber sovereignty. NUPI. Available at: https://www.jstor.org/stable/pdf/resrep07952.pdf?refreqid=excelsior%3A82b22d1f828031504a9dc41a53762715

[31] BBC (2015). Available at: https://www.bbc.co.uk/news/world-asia-china-35109453

[32] Schia, N. & Gjesvik, L. (2017).I

[33] Hoffmann, S., Lazanski, D. and Taylor, E. "Standardising the Splinternet: How China's technical standards could fragment the Internet." *Journal of Cyber Policy* (Forthcoming).

collecting and selling users' personal information without user consent.[34] The Chinese government is gradually introducing greater protections for user privacy and data, even while government surveillance increases.[35]

China is also attempting to build international consensus for its interpretation of digital sovereignty. Through the Shanghai Cooperation Organization (SCO), which also includes Russia, India, Pakistan and a number of Central Asian states, it advocates the primacy of the nation state over cyberspace.[36] China's state-led World Internet Conference has also provided a platform for China to promote a cyber-sovereign agenda.[37]

Also of note is China's Belt and Road Initiative, a project to connect Asia to Europe and Africa via a network of transport and telecommunications infrastructure. According to some estimates, China is engaged in around 80 telecommunications projects across the world.[38] Of particular relevance is the point that China's internet 'package' for developing nations also comes with systems, laws and training to apply the Chinese model of internet governance.

2.3 France

The French Senate has created an investigation committee on digital sovereignty, which published its conclusions on 3 October 2019. The report[39] defined digital sovereignty as the *"capacity of the state to act in cyberspace"*, along two dimensions. First, the ability to exercise sovereignty in the digital space and ensure cyber defence. Second, the ability to keep or restore French sovereignty over digital tools to be able to control French data, networks electronic communications.

The report gives five main recommendations:

- Define a national digital strategy within a temporary digital institutional forum
- Create a long-term framework for managing digital sovereignty by passing a law to approach and monitor it.
- Protect personal data and strategic economic data.
- Adapt regulation to digital challenges.
- Make use of the levers of innovation and multilateralism.

The report gives some observations about the current context in the following words[40]: *"The digital revolution and mastery of data has brought to the fore economic players that are capable of competing with the States."* Based on this context, it underlines that four domains are considered as being called into question: national defence, the legal order, the economic order and the fiscal and monetary system.

The French government has also created a €10 billion public fund – "public fund for innovation and industry" - to guarantee France's scientific and technological sovereignty as well as its economic development[41]. The French

[34] Sheng, W. (2019). One year after GDPR, China strengthens personal data regulations, welcoming dedicated law. Available at: https://technode.com/2019/06/19/china-data-protections-law/
[35] Sacks, S. and Laskai, L. (2019). China's Privacy Conundrum. https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html
[36] Schia, N. and Gjesvik, L. (2017).
[37] McKune, S. and Ahmed, S. (2018).
[38] https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next
[39] Book 1: http://www.senat.fr/rap/r19-007-1/r19-007-11.pdf - Book 2: http://www.senat.fr/rap/r19-007-2/r19-007-21.pdf
[40] October 2019: http://www.senat.fr/fileadmin/Fichiers/Images/redaction_multimedia/2019/2019_Infographies/20191004_infog_Souverainete_numerique_021019.pdf
[41] https://www.gouvernement.fr/le-fonds-pour-l-innovation

government has supported local innovation and assets in a range of digital areas seen as necessary to ensure digital sovereignty:

- **The Artificial Intelligence (AI) national strategy**, presented by the President of Republic on 29 March 2018, strongly embedded in a European framework, is based on 4 pillars[42]: strengthening the AI ecosystem to attract the best talent, developing an open data policy, creating a regulatory and financial framework that will foster the emergence of AI champions, and reflecting on AI regulation and ethics. As the President noted: *"For France and for Europe, this is a major issue of sovereignty: in AI, and more generally in all fields, there is a high risk of becoming dependent upon foreign technologies with no other choice than to use them under conditions established elsewhere. Worse still, to maintain our independence, we could be forced to deprive ourselves of major technological advances. When it comes to AI and all things digital, the State therefore needs to set itself the objective of reinforcing an industrial and technological base for the key sectors which are of strategic importance."*[43]

- **A Blockchain investment strategy** of €4.5 billion euros over five years was announced by the French Government in April 2019. France has passed the Pacte Act in the same period to set up a favourable legal framework[44] for crypto-assets service providers[45] and promote the development of blockchain.

- **Microelectronics**[46] is also supported for digital sovereignty issues, through the Leti/CEA Technology Research Institute.

- **Submarine cables**, through the negotiation between Nokia and the French government over the ownership of Alcatel Submarine Networks[47].

- **Cloud and cybersecurity** are also supported, as being tools for digital sovereignty, through the ANSSI, the National Agency for Information Systems Security (Agence Nationale de la Sécurité des Systèmes d'Information)[48].

In addition to the above, a law[49] was passed in France in July 2019 to establish a tax on digital services, primarily aiming at taxing global tech firms. The initial objective was to find a consensus at European level on common rules for determining the taxable base on profits, but unanimity could not be reached. Instead, France chose to introduce this tax in its national legislation, but it remains supportive of a cross-national approach to the issue.

2.4 Germany

The German government first set out in Leitplanken Digitaler Souveränität (Safeguards for digital sovereignty) (2015) its view on the key competencies necessary for German and European actors participating in the global digital economy to act in a sovereign manner. In this context, digital sovereignty designates the ability to self-determine in the domains of trade and decision-making within the digital space. More specifically, it refers to the ability to use commercial, scientific and community products, services, platforms and technologies such that:

[42] https://www.gouvernement.fr/argumentaire/intelligence-artificielle-faire-de-la-france-un-leader
[43] Page 37 For a meaningful artificial intelligence, towards a French and European strategy, Cédric Villani, a parliamentary mission from 8th Septembre 2017 to 8th March 2018
[44] https://www.gouvernement.fr/en/france-adopts-a-regulatory-framework-for-blockchains
[45] https://www.securities-services.societegenerale.com/en/insights/views/news/pacte-bill-french-regulatory-regime-crypto-asset-service-providers/
[46] Microelectronics is a branch of electronics concerning very small electronic components (Electronics cover the technologies - dealing with electrons - capable of electrical emission, flow and control. They include transistors, sensors, diodes, integrated circuits that are used to build electronic systems such as computers, IoT, Wi-Fi systems and smartphones.
[47] https://www.latribune.fr/technos-medias/souverainete-numerique-les-nuages-noirs-s-amoncellent-4-13-836810.html
[48] ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information); https://www.techinfrance.fr/cp-souverainete-numerique-et-cloud/; https://www.ssi.gouv.fr/actualite/campus-cyber-lambition-francaise-saffirme-pour-federer-et-faire-rayonner-lecosysteme-de-la-cybersecurite/
[49] Law No. 2019-759

- the users' security and privacy are not compromised;
- there is no unavoidable dependence, and
- the users' business ideas and models can be realised.

The concept of digital sovereignty became important in Germany due to the far-reaching influences that digital transformation has had in all walks of life and economy. The German state recognises the role of digital transformation in the creation of new products and services. Digital transformation also changes business models and firms' relationship with clients throughout the value chain. It is the view of the German government that digital sovereignty is key to the preservation of future competitiveness.

Leitplanken Digitaler Souveränität also presents concrete measures and recommendations for action that strengthen or reinstate digital sovereignty in Germany and Europe. The three main themes for these are capable and secure infrastructure, command of key competencies and technologies, and competitive innovation framework for digital sovereignty.

Digital sovereignty was further examined in the specific context of artificial intelligence in 2018 in the paper Digitale Souveränität und Künstliche Intelligenz – Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen (Digital sovereignty and Artificial Intelligence – Prerequisites, Responsibilities and Recommendations for Action). Germany believes artificial intelligence to be the future general-purpose technology. It is therefore necessary to ensure that political and administrative, techno-economic, as well as scientific and research frameworks exist that underpin the various competencies needed to achieve digital sovereignty as defined in the first paragraph.

The 2018 paper goes further than the 2015 paper and recommends a layer model for assessing the degree of digital sovereignty. The assessment is based on a definition of what it means to have a high degree of digital sovereignty. The definition gives the necessary conditions for the presence of high level of digital sovereignty, and these conditions are the bases for the assessment guidelines.

Another paper in the same vein as the 2018 paper on artificial intelligence is Digitale Souveränität im Kontext plattformbasierter Ökosysteme (Digital sovereignty in the context of platform-based ecosystem). This deals with digital sovereignty in the context of platform-based ecosystems and provides a similar layer model for assessing the degree of digital sovereignty. The paper raises the need for platform users (including individuals, government authorities and enterprises) to cultivate digital sovereignty on the one hand and the need for the country to build the capacity required to develop and operate its own digital platform on the other hand. This is due to the growing influence of digital platforms on the ability of the state, companies, and society to communicate and be innovative. Recommendations for action are made on regulations, cooperation models between competitors amongst other things.

The general approach to digital sovereignty in Germany has, therefore, been one of determining the competencies required to achieve digital sovereignty and the resulting conditions. In addition to the government's papers above, a government department released a similar publication in the context of consumer protection in 2017. Recommendations are provided in this paper in the areas of technology, digital literacy and regulations, which are aimed at fostering the right conditions for digital sovereignty for consumer market.[50]

[50] Available at: http://www.svr-verbraucherfragen.de/wp-content/uploads/English-Version.pdf

One notable measure is Germany's plans to create a cloud service to provide European companies with an alternative to US or Asian rivals. This service, dubbed Gaia-X, is intended to provide a joint European standard for data sharing, and to provide Europe with a data infrastructure that *"ensures data sovereignty*".[51]

Even though digital sovereignty is viewed as integral to economic success, absolute digital sovereignty is not the goal[52]. The German government recognises that it is not possible and also not worthwhile in many cases to attain full digital sovereignty, since a high degree of digital sovereignty can be associated with great effort and costs. For example, the use of some off-the-shelf "Software as a Service (SaaS)" may lead to transfer of personal data and dependence on the vendor in such a way that digital sovereignty is reduced. The alternative, however, is a proprietary system, over which one has full control. The higher level of digital sovereignty achieved in this way is associated with additional effort for setting up, secure operation and possibly even the further development of self-operated solutions.[53]

2.5 India

The Indian government's approach to digital sovereignty is primarily focused on data sovereignty – ensuring adequate protections for Indian users and ensuring that personal data is stored in-country.

The drive towards greater data sovereignty was given impetus by the Cambridge Analytica revelations 2018 case - the Indian government has claimed that out of the 87 million users' data transferred by Facebook to Cambridge Analytica, 500,000 were Indian.[54] As a result, the Indian government started a consultation process with the key stakeholders to come up with a data protection policy. The objectives of this policy were to unlock the potential of the digital economy for India, to protect the personal data of Indian citizens, and to protect them from the state's unregulated control of their data.[55]

The final output of these consultations is the Data Protection Bill 2019, introduced in the Indian parliament in December last year. It is scheduled to be debated upon in the upcoming parliament session in July-September 2020 before it can become a law. The bill seeks to protect the personal data of individuals and establish a Data Protection Authority to do the same. Under the bill, the individuals have a right to know whether their personal data has been processed, seek correction, transfer data, and restrict disclosure of their personal data.[56]

The bill governs the processing of personal data by the government, companies incorporated in India, and foreign companies dealing with personal data of individuals in India. These entities are obliged to process the collected data only with prior individual consent and for a specific and lawful purpose. They are also tasked to set up transparency and accountability measures to address individual complaints.[57]

[51] Jennen, B. and Nicola, S. (2019). Germany to Unveil European Cloud to Rival Amazon, Alibaba. *Bloomberg*. Available at: https://www.datacenterknowledge.com/europe/germany-unveil-european-cloud-rival-amazon-alibaba

[52] Here, a full digital sovereignty (Eine vollständige digitale Souveränität) refer to a situation where an actor ensures that they have full control of all digital assets through self-provision. Though this gives them absolute autonomy, the cost of gaining such control would be extortionate.

[53] https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5

[54] Committee of Experts under the chairmanship of B.N. Sri Krishna, 2018, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. Available at: https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018_0.pdf

[55] Committee of Experts under the chairmanship of B.N. Sri Krishna, 2018, A Free and Fair Digital Economy Protecting Privacy, Empowering Indians. Available at: https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018_0.pdf

[56] PRS Legislative Research (2019). Bill Summary: The Personal Data Protection Bill. Available at: https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%202019%20PRS%20Bill%20Summary.pdf

[57] Ibid.

The bill also includes a requirement for data localisation of sensitive personal data. The bill defines sensitive personal data[58] to include financial data, biometric data, caste, religious or political beliefs. As per the bill, sensitive personal data should be stored in India and can only be transferred outside India with the explicit consent of the individual.[59]

The Indian government views the data localisation requirements as a necessity to respond to foreign tech companies generating revenue from the data of the Indian citizens. This phenomenon is also referred to as data colonialism by some local industrialists, academic and civil society actors, and politicians.[60] This stance is supported by domestic civil society and big private players in India like the Reliance Jio and Paytm. However, there has been criticism from smaller digital players that data localisation would mean increased compliance costs. Data localisation could also have trade policy implications if other countries impose reciprocal measures.[61,62]

In addition to the Data Protection Bill 2019, the draft e-Commerce Policy 2019 also promotes data localisation by restricting the cross-border flow of data generated by Indian users from sources like e-commerce platforms, social media, and search engines.[63] Data collected by IoT devices installed in public places is similarly restricted, but may be shared with domestic entities for research purposes. The government plans to prioritise the sharing of anonymised data with Indian start-ups and enterprises to boost innovation and economic growth in the country.

A further contentious provision of the Data Protection Bill 2019 relates to the discretion provided to the government to exempt any government agency or department from the purview of the bill on grounds of national security, public order, sovereignty and integrity of India and friendly relations with foreign states. This has raised concerns that the government might use this provision to expand surveillance on its citizens.[64]

2.6 Russia

Russia is one of the world's strongest advocates for national sovereignty over cyberspace. Together with China, it has consistently argued for a greater role for national governments in internet governance in international forums,[65] and has (along with China and several Central Asian states) proposed two Codes of Conduct on Information Security at the UN General Assembly.[66]

Russia does not exercise the same control of its domestic cyberspace and historically has much closer ties with the development of today's global internet. However, it is taking steps to tighten its control. In November 2019 the "sovereign internet" law came into force, requiring ISPs to be able to route the country's web traffic through state-controlled points (which would also enable monitoring and filtering of the traffic).

[58] All existing categories of sensitive personal data according to India's Data Protection Bill include financial data, health data, official identifier; sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation.
[59] PRS Legislative Research (2019). Bill Summary: The Personal Data Protection Bill. Available at: https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%202019%20PRS%20Bill%20Summary.pdf
[60] The Centre for Internet and Society (2019). The Localisation Gambit: Unpacking policy measures for Sovereign control of Data in India. Available at: https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf
[61] Ibid.
[62] Internet & Jurisdiction Policy Network (2019). India: Proposed E-Commerce Policy calls for increased data localization and increased protection of data privacy and consumer rights. I&J Retrospect Database. Available at: https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaW5kaWEiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9
[63] The Centre for Internet and Society (2019). The Localisation Gambit: Unpacking policy measures for Sovereign control of Data in India. Available at: https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf
[64] The Economic Times (2019). Personal Data Protection Bill can turn India into "Orwellian State": Justice BN Srikrishna. Available at: https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?from=mdr
[65] For example, in ITU summits. See above.
[66] Broeders, D., L. Adamson and R. Creemers. (2019). Coalition of the unwilling? Chinese and Russian perspectives on cyberspace. The Hague Program For Cyber Norms Policy Brief. November 2019., Available at SSRN: https://ssrn.com/abstract=3493600

Russia is also working on creating its own version of the Domain Name System (DNS) so that it can operate practically autonomously. This would give Russia the power to isolate its internet from the global internet, though Russia's network infrastructure means that in practice this would be expensive and technically difficult[67].

Another law, requiring foreign smart devices sold in Russia to come pre-installed with a suite of apps, is due to come into force in July 2020. One of the bill's co-authors argued that the purpose of the law is to encourage the use of Russian alternatives to preinstalled (and generally Western) apps, though it could also facilitate surveillance of users.[68] This law led to speculation that Apple – which does not allow third party software to be preinstalled – could withdraw from the Russian market.[69]

These laws are part of a series of regulations relating to cyberspace, which include implementing punishments for disrespecting the state or spreading fake news, data localisation requirements, requiring messaging services to share encryption keys with security services,[70] and restrictions on virtual private networks (VPNs).

2.7 United States

The US has no clearly stated position on digital sovereignty. This is likely because of its privileged position in the digital economy: many major tech firms are based in the USA, and users and other actors in the digital value chain are dependent on them. Indeed, it is at least partly in response to US tech hegemony that other states are pursuing greater digital sovereignty.

The White House recognises, however, that there are other threats which can undermine its current advantageous position. The key threat highlighted in its National Cyber Strategy, published in 2018, is the threat to cybersecurity.[71] The security of cyberspace is viewed as fundamental to the protection of America's national security and promoting the prosperity of its people because cyberspace is integral to all facets of American life. The USA believes that there are states and individuals intent on carrying out malicious activities that will compromise the cyberspace.

One of the US's key plans is to model and promote standards that would protect American economic security and reinforce the vitality of its marketplace and innovation. This involves prioritising innovation, investing in next generation infrastructure, promoting the free flow of data across borders, and maintaining its leadership in emerging technologies. In other countries, these actions will help to create the conditions necessary for digital sovereignty. They are intended to help preserve America's position in the digital economy.

The US also sets as its objective the preservation of long-term openness, interoperability, security, and reliability of the Internet to support the United States' interests and values. Key actions for this objective include protecting and promoting internet freedom, promoting the current multistakeholder model of internet governance, and promoting and maintaining markets for United States firms worldwide. A further objective is to push back against the creation of state-centric frameworks that remove users' freedom of choice over the Internet.

While the US does not have an explicit digital sovereignty stance, it has pursued a sovereign agenda in related areas. One example is the US Cloud Act, which authorises US law enforcement to demand access to data held by US companies overseas. The act, and a related US-UK bilateral agreement to allow cross-border data access

[67] Musiani, F. et al (2019). 'Digital sovereignty': can Russia cut off its Internet from the rest of the world? Available at: https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-internet-from-the-rest-of-the-world-125952
[68] BBC (2019). Available at: https://www.bbc.co.uk/news/world-europe-50507849
[69] Nadeau, J. (2020). Apple has a Vladimir Putin problem. Available at: https://www.fastcompany.com/90456530/apple-has-a-vladimir-putin-problem
[70] The Moscow Times (2019). Putin Signs 'Fake News,' 'Internet Insults' Bills Into Law. Available at: https://www.themoscowtimes.com/2019/03/18/putin-signs-fake-news-internet-insults-bills-into-law-a64850
[71] National Cyber Strategy of the United States of America (2019). https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

by law enforcement, has come under criticism from privacy advocates.[72] There are also concerns about how the Act will interact with data protection measures imposed by other states, such as GDPR.[73]

[72] EPIC. The Cloud Act. Available at: https://epic.org/privacy/cloud-act/
[73] 1&1 IONOS (2019). The Controversial Cloud Act. White Paper. Available at: https://www.ionos.co.uk/digitalguide/websites/digital-law/cloud-act/

3 Enterprise

Compared to efforts in support of digital sovereignty for national and regional governments, non-state actors seem to play a far smaller role. In fact, enterprises and businesses are rarely mentioned as entities that have digital sovereignty concerns or aspirations. In the face of virtualization and cloud computing, enterprises may choose to store data, process it and report upon it outside of the enterprise's network boundaries. In addition, many businesses use third parties to collect and process data about the operations and management of the company.

For enterprises the focus of digital sovereignty often circles around how the enterprise can ensure that they are in control of the creation, storage and processing of their data.

An example is precision agriculture: the practice of using a segmented management approach where crop production is tailored to meet the unique needs of each individual segment of land.[74] The basic idea of precision agriculture is to collect data and make decisions based on that data. This idea has been around for many years.[75] Agricultural data is collected in the field and sent directly to an agricultural technology Provider (ATP). The ATP may offer to provide storage for the producer's data. It may also offer to conduct analysis of the data and provide agricultural advice for a fee.[76]

Agricultural data of this kind is economically valuable. An agricultural technology provider could use data, collected from multiple producers, to develop new products to sell and significantly increase their own profits.[77] Options and commodity traders could gain advantage in the market by using the data to influence decisions made in the stock and commodity markets. In the end, the agricultural enterprise stands at risk of losing the value of the data extracted from the farm.

Precision agriculture is only an example of how an enterprise can utilise data. In a research paper from 2018, Deloitte calls enterprise data sovereignty the ability to "develop deliberate techniques for managing, monetizing and unlocking the value of an increasingly vital enterprise asset.[78]" The Deloitte paper stresses internal use of the enterprise's data and stresses that a business needs to solve problems in data management and architecture, global regulatory compliance and data ownership. Thus, *enterprise data sovereignty* has very different aims than state-oriented discussions of data sovereignty.

For contemporary enterprises, data sovereignty is a strategy for an organization to inventory its data, make that data available and consistent, and control where the data is stored and who has access to it. When we talk about enterprise digital sovereignty, there are two major market segments affected by the issue. For consumers, the primary issue is privacy (see Section 5). However, for enterprises, the main issues are security and control of the value of the data. Loss of control of the data can lead to asymmetrical acquisition of information by third parties. As with consumer data, this has economic impacts far beyond a single business or enterprise. For the enterprise, information is an asset. Combined with algorithms, the asset has additional value, both inside the enterprise and for customers outside the enterprise.[79]

[74] Hart, J. (2015). Efficiency, Accuracy Biggest Advantages of Precision Agriculture. *Southeast Farm Press.* Available at: http://southeastfarmpress.com/management/efficiency-accuracy-biggest-advantages-precision-agriculture
[75] History of Precision Agriculture. Available at: http://www.delmarlearning.com/companions/content/140188105X/trends/history_pre_agr.asp.
[76] Agrimarketing (2015). Startups, Major Agribusinesses Compete in Big Data Market Space. http://www.agrimarketing.com/s/98423
[77] Bunge, J. (2014). Big Data Comes to the Farm Sowing Mistrust. *Wall Street Journal.* Available at: http://www.wsj.com/articles/SB10001424052702304450904579369283869192124
[78] Deloitte Insight (2020). Enterprise data sovereignty: if you love your data set it free. Available at: https://www2.deloitte.com/us/en/insights/focus/tech-trends/2018/data-sovereignty-management.html
[79] Demchenko, Y. et al (2018). Data As Economic Goods. ITU Journal, ICT Discoveries, Special Issue No. 2 November 2018, https://www.itu.int/en/journal/002/Documents/ITU2018-12.pdf

For enterprises, data sovereignty is one component of digital sovereignty. It includes the collection of data, its integration with other sources of data, analysis, and applying the results to data driven services.[80] To understand enterprise data sovereignty, it is crucial to understand the differences between data sovereignty, data residency and data localization. Data residency is simply the situation where a business, industry body or government specifies that data must be stored in a specific geographic location. Data sovereignty goes beyond data residency by requiring the data to be stored in a designated location and also being subject of the laws of the country in which it is physically stored. Data localization goes beyond data sovereignty by requiring that data created within certain borders, stay within those borders.

Enterprises are unlike states and citizens in that their digital sovereignty issues relate to an organization's self-sufficiency and control over its digital infrastructure and its approach to data sovereignty. Multinational enterprises concern themselves with the security, regulatory, legal and trust components of its infrastructure. Multinationals also must deal with the regulatory and legal consequences of its data infrastructure. Enterprises in a single country potentially have less complex regulatory and legal issues to deal with.

For data sovereignty, we are just beginning to see frameworks for usage control and trust management systems of inter-enterprise data exchange.[81] This means that some of the key enterprise digital sovereignty for information sharing, value generation and security can be dealt with in a framework that includes data providers, data enhancers and data consumers.[82]

[80] Unal, P. Reference Architectures and Standards for the Internet of Things and Big Data in Smart Manufacturing. 7th International Conference on Future Internet of Things and Cloud, https://www.researchgate.net/profile/Perin_Unal/publication/335430231_Reference_Architectures_and_Standards_for_the_Internet_of_Things_and_Big_Data_in_Smart_Manufacturing/links/5d653ebd299bf1f70b10322e/Reference-Architectures-and-Standards-for-the-Internet-of-Things-and-Big-Data-in-Smart-Manufacturing.pdf

[81] Zrenner, J., Möller, F.O., Jung, C., Eitel, A. and Otto, B. (2019), "Usage control architecture options for data sovereignty in business ecosystems", Journal of Enterprise Information Management, Vol. 32 No. 3, pp. 477-495. https://doi.org/10.1108/JEIM-03-2018-0058

[82] Bellanger, P. (2012). De la souveraineté numérique. *Le Débat*, vol. no 170, no. 3, 2012, pp. 149-159.

4 Citizens and civil society

Much of the public discussion around digital sovereignty focuses on industry and government – more recently highlighting the collision between the two, such as the Snowden revelations[83], Cambridge Analytica[84] scandal, and moves to regulate online spaces. As the internet grows and evolves, impacting everyday lives, citizens are becoming more aware of potential abuses and misuses of their information or the impact of digital divides and the subsequent harms these can cause – for example, to their safety, access to basic service, and human rights. In the context of *citizens' digital sovereignty*, more recently, this has led to a greater focus on right to ownership and control over personal data and offsetting potentially negative impacts of emerging technologies.

Citizens and civil society[85] are in a difficult position because their digital sovereignty often intersects with, and can put citizens at odds with, the state and/or enterprises – in particular the tech and advertising[86] industries. At the same time, to enact serious change partnership, or at least cooperation, between citizens and either government (including its formal mechanisms like the rule of law) or industry is often required. As a result, their toolbox for exercising digital sovereignty ranges from legal action to more inventive technical means.

The currency by which users are now accessing services and applications is not financial, but by trading their own data. Enterprises feed off of data. They mine as much data as possible about users to not only develop better systems or services, but to monetise it through sale to marketers, developers, or data brokers, and possibly even shape citizens' future behaviour.[87]

Personal data is both a raw material and revenue generator, and users are becoming increasingly aware of the ways in which personal data lives on in digital environments.[88] In Europe, this was assisted by well reported court cases. For example, a case brought against Google Spain in the European Court of Justice now known for producing the 'Right to Be forgotten'.[89] This landmark case showed the power of citizens to use existing legal frameworks to protect their public image and control their digital footprint.

Other high-profile court cases resulted in fundamental changes to the data transfer relationship between the EU and US. The case Maximillian Schrems v. Data Protection Commissioner[90] resulted in a new agreement, *Privacy Shield*, developed alongside the General Data Protection Regulation (GDPR). Both frameworks aimed to provide users more information about personal data collection, use, and ability to claim more control – key elements of digital sovereignty. For instance, both set out requirements to inform users about the type, purpose, and transfer of data to third parties, and notification of data breaches.

However, mechanisms such as *Privacy Shield* are contentious because national laws can influence protection (and disclosure) mechanisms as data is transferred across borders. As a result, in July 2020 the European Court of Justice struck down *Privacy Shield* due inadequate protection under and the potential impact of US national security laws on personal data.[91]

[83] Macaskill, E. and Dance, G. (2013). NSA files: decoded – what the revelations mean for you. Available at: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded
[84] Wong, J. (2019). The Cambridge Analytica scandal changed the world – but it didn't change Facebook. Available at: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook
[85] Jezard, A. (2018) . Who and what is civil society? Available at: https://www.weforum.org/agenda/2018/04/what-is-civil-society/
[86] BBC (2019). Who's making money out of your data? Available at: https://www.bbc.co.uk/news/av/entertainment-arts-49495445/who-s-making-money-out-of-your-data
[87] Naughton, J. (2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. Available at: https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook
[88] Internet Society. Your digital footprint matters. Available at: https://www.internetsociety.org/tutorials/your-digital-footprint-matters/
[89] Court of the European Union (2014. Press Release No 70/14. Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf
[90] Judgment of the Court (Grand Chamber) of 6 October 2015. Case C-362/14. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362
[91] BBC (2020). EU-US Privacy Shield for data struck down by court. https://www.bbc.co.uk/news/technology-53418898

In contrast to that of enterprises, part of a state's role is to protect its citizens from harm and uphold basic human rights. For some citizens, the collection and use of data by states, particularly within scope of relevant regulations and for the benefit of society, does not pose significant issue. Thus, a process of bargaining data for public services is a part of a citizen's digital sovereignty. Nevertheless, new uses and collection of data is still of concern. More recently, the development and potential adoption of COVID-19 tracking apps in Europe have sparked heavy debate among government and privacy advocates[92] and resulted in pre-emptive attempts by the European Union to set out expectations of data management and protection.[93]

State accountability and transparency are often expected by citizens as a sort of checks-and-balances approach. In the event of perceived overstep, in many countries citizens can and do take collective legal action to exercise their digital sovereignty. For instance, the numerous court cases brought against the UK government following the Snowden revelations for unwarranted mass surveillance – or collection, retention and processing – of phone and internet data.[94,95] The result has been ongoing cases in the European Court of Human Rights (ECHR) (currently now in the Grand Chamber).[96] It also had broader implications on policy development within the UK, particularly on the Investigatory Powers Act (2016) due to related appeals brought forward by Members of Parliament.[97]

However, in some states the lack of due process or other government accountability mechanisms often leave citizens with fewer options to exercise digital sovereignty. For example, in Saudi Arabia where the government uses advanced Internet filtering tools[98] users trying to circumvent such restrictions often adopt anti-filtering tools, or, if able, purchase devices and apps when outside the region to avoid local market regulations. In China, there is a web of government surveillance and censorship[99] tools that citizens navigate on a daily basis using self-censorship and privacy protecting tools[100] such VPNs and the Tor browser.[101] But citizens have also devised some interesting ways to communicate. For example, to circumvent China's content filters, citizens have learned to communicate in emojis[102], analogies, and homophones[103].

As technology evolves so too do the concerns of citizens over their digital sovereignty. Unfortunately, the speed of technological evolution at this time is such that citizens are usually on the back foot. With the slow rollout of 5G civil society organisations are trying to get in front of the curve of this game-changing networking technology and their concerns for human rights such as privacy[104] and freedom of expression. The non-governmental organisation Privacy International has published 5G explainers and recommendations for corporations and governments to ensure use is privacy respecting[105], and the Article 19 organisation is pushing

[92] Human Rights Watch (2020). Covid-19 Apps Pose Serious Human Rights Risks. https://www.hrw.org/news/2020/05/13/covid-19-apps-pose-serious-human-rights-risks
[93] EDPB (2020) .adoptedGuidelines04/2020onthe use of location data and contact tracing tools in the context of the COVID-19 outbreak https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf
[94] Privacy International (2018). Fighting Mass Surveillance in the Post-Snowden Era. https://privacyinternational.org/node/2602
[95] Privacy International (2018). Press release: Campaigners win vital battle against UK mass surveillance at European Court of Human Rights. https://privacyinternational.org/press-release/2265/press-release-campaigners-win-vital-battle-against-uk-mass-surveillance-european
[96] Big Brother Watch (2019). UK mass surveillance challenged in Europe's highest human rights court. https://bigbrotherwatch.org.uk/2019/07/uk-mass-surveillance-challenged-in-europes-highest-human-rights-court/
[97] Haydock, A (2018). The latest ruling against the Snooper's Charter is welcome, but the Courts need to do more. https://www.openrightsgroup.org/blog/liberty-snoopers-charter-decision/
[98] OpenNet Initiative. Internet Filtering in Saudi Arabia in 2004. https://opennet.net/studies/saudi
[99] Garber, M. (2014). There Are 64 Tiananmen Terms Censored on China's Internet Today. Available at: https://www.theatlantic.com/technology/archive/2014/06/china-has-found-64-tiananman-related-terms-to-block-on-its-internet-today/372137/
[100] Cunningham, L. (2019). Countering Chinese Censorship. Available at: https://www.usagm.gov/2019/08/08/countering-chinese-censorship/
[101] Freedom House (2019). Country Profile – China. Available at: https://freedomhouse.org/country/china/freedom-net/2019
[102] Hernández, J. (2020). As China Cracks Down on Coronavirus Coverage, Journalists Fight Back. Available at: https://www.nytimes.com/2020/03/14/business/media/coronavirus-china-journalists.html
[103] Si, J. (2017). The Chinese Language as a Weapon: How China's Netizens Fight Censorship. Available at: https://medium.com/berkman-klein-center/the-chinese-language-as-a-weapon-how-chinas-netizens-fight-censorship-8389516ed1a6
[104] FitzGerald, D. (2019). 5G Race Could Leave Personal Privacy in the Dust. *Wall Street Journal.* https://www.wsj.com/articles/5g-race-could-leave-personal-privacy-in-the-dust-11573527600
[105] Privacy International (2019). Welcome to 5G: Privacy and security in a hyperconnected world (or not?). https://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not

for 5G to include human rights discussions from the outset of technology[106] and policy[107] development. Some regulatory bodies are taking note of these concerns.[108, 109]

Algorithms[110] have also become an important topic for citizens, particularly with the increasing use of AI and machine learning. Algorithms have the potential to modify themselves as it 'learns' and adapts its processes. Yet ultimately, human decisions have a significant impact on an algorithm's functioning, with many pointing to developer bias inherently built into a system that claims to be agnostic or neutral.[111] This is fundamental to the call by civil society for algorithmic transparency and 'ethical', 'trustworthy', and 'fair' algorithms.

Citizen groups like AI Now work on not only the ethical and policy considerations, but develop toolkits for policymakers and industry.[112] Newer legislation, such as GDPR has taken on board some of civil society's concerns by setting out provisions on automated decision making.[113] Governments, enterprises, and citizens each have their own interest in the development and use of algorithms. Some legal systems are also taking on board citizen concern regarding algorithms in their reviews of algorithms used in legal contexts. For instance, the UK's Law Society published a report on the use of algorithms in the criminal justice system, finding not only that the use of algorithms lack openness and transparency, but some uses today 'lack a clear and explicit lawful basis'.[114]

[106] Article 19 (2016). Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite? Available at: https://www.article19.org/resources/our-5g-future-light-at-the-end-of-the-tunnel-or-internet-fast-lane-for-the-elite/

[107] Article 19 (2019). BEREC: Freedom of expression must be guaranteed in regulation of electronic communications markets. Available at: https://www.article19.org/resources/berec-freedom-of-expression-must-be-guaranteed-in-regulation-of-electronic-communications-markets/

[108] BEREC (2019). Report on the impact of 5G on regulation and the role of regulation in enabling the 5G ecosystem. https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8910-report-on-the-impact-of-5g-on-regulation-and-the-role-of-regulation-in-enabling-the-5g-ecosystem

[109] Wong, S. (2019). Personal Data Privacy Implications of 5G Technology. Available at: https://www.pcpd.org.hk/english/news_events/whatison/files/5g_12112019.pdf

[110] Defined as *"a documented series of steps which leads to the transformation of some data"*. See https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095402315

[111] Hao, K. (2019). This is how AI bias really happens—and why it's so hard to fix. *MIT Technology Review.* Available at: https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/

[112] AINow Institute (2018). Algorithmic Accountability Policy Toolkit. Available at: https://ainowinstitute.org/aap-toolkit.pdf

[113] Information Commissioner's Office (UK). Rights related to automated decision making including profiling. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

[114] The Law Society (2019). Algorithm use in the criminal justice system report. https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/

5 The future of digital sovereignty

A diversity of national approaches

As noted in Section 3, there is a growing political appetite from governments to intervene in cyberspace. Many states are developing or implementing policies and initiatives to regulate various facets of cyberspace, such as hate speech, data privacy and data localisation. Many are also looking to increase their digital autonomy by encouraging their domestic tech sectors and emerging technology areas such as artificial intelligence. Some states are also reluctant to participate in internet governance conventions on the grounds that they were not engaged from the outset – for example, India and the Budapest Convention on cybercrime.[115]

These policy approaches are typically developed at the national level, resulting in an increasingly diverse set of rules and regulations. As noted by the Internet and Jurisdiction Policy Network, *"nation states with different visions are seeking to increase their control over the internet, primarily by using national tools rather than transnational cooperation and coordination"*.[116] This is resulting in growing regulatory and technical fragmentation of the global internet – a process dubbed "digital Balkanization" or the "splinternet"[117] – which threatens the cross-border nature of today's internet.

This process is likely to have a number of implications:

- **An increase in cross-border legal challenges**. Regulations defined at a national level - for example, extraterritorial assertions of jurisdiction (such as in the case of access to data) - may bring states' interpretation of digital sovereignty into conflict. According to a stakeholder survey, 95% see cross-border legal challenges on the internet becoming increasingly acute in the next three years.[118]

- **An increase in compliance costs for online business.** Online businesses must ensure compliance with a growing set of national regulations, resulting in higher costs. For example, Google has around 100 staff working to ensure compliance with Germany's NetzDG law; Facebook has 65 staff and Twitter 50 staff.[119]

- **Loss of cross-border benefits.** The global nature of the internet has led tech firms to structure their operations to reduce costs. For example, the Nordic countries are home to numerous data centres due to the low cost of energy and colder climate.[120] Data localisation requirements, such as those under consideration in India, would mean sensitive data must be stored in-country, resulting in more numerous (and less efficient) data centres.

- **Data flows.** A varied array of data protection and privacy regulation may inhibit the scope for data transfer across borders. This may create new barriers to research and cross-border applications, as well as emerging areas such as machine learning.

- **Threats to freedom of expression.** Certain regulations may reduce freedom of expression, for example, limiting access to services provided by overseas firms in favour of local state-controlled firms.

[115] Seger, A. (2016). India and the Budapest Convention: Why not? *Observer Research Foundation.* Available at: https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/
[116] Internet Jurisdiction and Policy Network (2019). Internet and Jurisdiction Global Status Report 2019. Available at: https://www.internetjurisdiction.net/uploads/pdfs/GSR2019/Internet-Jurisdiction-Global-Status-Report-2019_web.pdf
[117] Financial Times (2019). Europe should not be afraid of the 'splinternet'. Available at: https://www.ft.com/content/e8366780-9be5-11e9-9c06-a4640c9feebb
[118] Internet Jurisdiction and Policy Network (2019).
[119] Echikson, W, and Knodt, O. (2018). Germany's NetzDG: A key test for combatting online hate. *CEPS*. Available at: http://wp.ceps.eu/wp-content/uploads/2018/11/RR%20No2018-09_Germany's%20NetzDG.pdf
[120] Lima, J. (2020). Hot Nordic. The cold land where data centre investments are heating up. Available at: https://data-economy.com/hot-nordic-the-cold-land-where-data-centre-investments-are-heating-up/

The rule of the strongest?

One potential consequence of a fragmented global internet could be the entrenchment of global hegemons – where the rules of the game are set by and for large actors. One clear example of this is in the extraterritorial application of laws, which larger states have much greater power to enforce. This brings into question just how effective data localisation requirements might be, if powerful nations can compel tech companies to hand over any data that they control.

Another example might be the race to connect users in developing countries. For instance, China is investing in African countries' internet infrastructure, using Chinese products and standards.[121] Google and Facebook are also racing to connect users in developing countries – Facebook has connected around 100m in 60 countries through its Free Basics scheme, while Google is deploying balloon-based connectivity through its Project Loon.[122]

These schemes may give powerful states and tech firms a significant influence on digital policy in developing countries that cannot afford to say no.[123] This raises questions about just how much latitude those countries will have to forge an independent digital sovereignty policy.

Tech giants can use their global clout to influence policy and may even threaten withdrawal of service to protest regulations they dislike - in 2014, Google shut down its Google News service in Spain (a relatively large market of 46m) in protest against a new law – the "snippet tax"[124] (a similar battle is now brewing in France[125]). Threats to withdraw popular services could be a powerful negotiating tactic, particularly in smaller markets, but may also open these markets to local competitors struggling to attract user attention (and thus support states' digital sovereignty through indigenous technology).

For some developing nations, the open Internet may appear to be little more than a vehicle for 'digital colonisation' by the global tech giants.[126] Some have also argued that their ability to influence the current multistakeholder model is limited.[127] For many such nations, the prospect of Chinese infrastructure investment is likely to be attractive, even if it does mean de facto adoption of Chinese internet norms and practices.[128,129] Indeed, the level of control offered by the Chinese model may be attractive to some.

The export of the Chinese model of internet governance via the Belt and Road Initiative led former Google CEO Eric Schmidt to predict a 'bifurcation' of the global internet into a Chinese-led internet and non-Chinese internet.[130] If the Chinese model gains enough traction it may become large enough to be economically self-sustaining in isolation. A more likely scenario, however, is that a level of interoperability would be maintained to allow some access to the global internet economy.

A key distinction between the multistakeholder model and state-led internet governance models is that the former allows the participation of a range of different actors, including private companies and civil society.

[121] Internet Jurisdiction and Policy Network (2019). p64
[122] Reynolds, M. (2019). Facebook and Google's race to connect the world is heating up. Available at: https://www.wired.co.uk/article/google-project-loon-balloon-facebook-aquila-internet-africa
[123] India's telecoms regulator did in fact ban Facebook's Free Basics service in 2016, but smaller countries may be unwilling or unable to do the same.
[124] Benton, J. (2019). Google is threatening to kill Google News in Europe if the EU goes ahead with its "snippet tax". https://www.niemanlab.org/2019/01/google-is-threatening-to-kill-google-news-in-europe-if-the-eu-goes-ahead-with-its-snippet-tax/
[125] Lomas, N. (2020). France's competition watchdog orders Google to pay for news reusehttps://techcrunch.com/2020/04/09/frances-competition-watchdog-orders-google-to-pay-for-news-reuse/
[126] Adee, S. (2019). The global internet is disintegrating. What comes next? *BBC Future.* Available at: https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next
[127] Thimm, J. and Schaller, C. (2014). Internet Governance and the ITU: Maintaining the Multistakeholder Approach. Available at: https://www.cfr.org/report/internet-governance-and-itu-maintaining-multistakeholder-approach
[128] El Hadi, T. (2019). The Promise and Peril of the Digital Silk Road. Available at: https://www.chathamhouse.org/expert/comment/promise-and-peril-digital-silk-road
[129] Gagliardone, I. (2013). Is China shaping the Internet in Africa? Available at: https://blogs.oii.ox.ac.uk/policy/is-china-shaping-the-internet-in-africa/
[130] Kolodny, L. (2018). Former Google CEO predicts the internet will split in two — and one part will be led by China. *CNBC.* https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html

Fragmentation of the global internet into regional blocs could mean that the rules of the game are instead defined largely by powerful states. This path may also bring risks, such as the economic impact of being excluded from a global internet, or a chilling effect on freedom of expression.[131]

A return to multistakeholderism?

The increasing divergence of national rules and regulations concerning the internet has prompted some to argue for a new system of global governance to preserve the cross-border internet. In 2019, the Internet and Jurisdiction Policy Network hosted 200 stakeholders from states, industry and civil society at a conference to discuss how to encourage internationally coherent internet policy.[132]

The challenge comes in allowing states to apply their own national rules to the internet while maintaining the global nature of the internet. One way forward is the development of a common interpretation of legal concepts to increase 'legal interoperability' and the coordination of national policy.[133] Others have called for international regulation, though this will likely take years.[134]

While this goal seems like a long shot, there may still be some grounds for optimism. Many of the internet's benefits come from its global, cross-border nature, facilitated by flexible, interoperable technologies and international multistakeholder governance. States will be reluctant to entirely exclude themselves from those, no matter how great their desire for control over the internet. As observers have noted, while there *is* fragmentation of the global internet, closed "sovereign" networks are unlikely to emerge.[135][136]

Even China, the furthest along that road, sees the economic benefits of, for example, multinational cloud service providers[137] and of maintaining interoperability between its tech sector and global cyberspace.[138] It remains to be seen whether the draw of economic self-interest will be enough to avoid further splits in the global internet.

[131] Dutton, W. et al (2011). The Changing Legal and Regulatory Ecology Shaping the Internet. Available at: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-internet/

[132] Scott, M. (2018). The internet is broken. Can this group fix it? *Politico EU.* Available at: https://www.politico.eu/article/internet-governance-ottawa-regulation-balkanization-splinternet-global-jurisdiction-policy-network/

[133] Internet Jurisdiction and Policy Network (2019).

[134] Scott, M. (2018).

[135] Cattaruzza, A. et al (2016). Sovereignty in Cyberspace: Balkanization or Democratization. *2016 IEEE International Conference on Cyber Conflict (CYCON U.S.).* Available at: https://www.academia.edu/31828716/Sovereignty_in_Cyberspace_Balkanization_or_Democratization

[136] Polatin-Reuben, D. & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. Available at: https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf

[137] Ibid.

[138] Broeders, D. et al. (2019). A coalition of the unwilling Chinese and Russian perspectives on cyberspace. *The Hague Program for Cyber Norms.* Available at: https://www.thehaguecybernorms.nl/research-and-publication-posts/a-coalition-of-the-unwilling-chinese-and-russian-perspectives-on-cyberspace

Appendix A About the authors

Sam Wood is a Principal at Plum. An economist by training, he has worked on numerous studies related to digital regulation, policy and the digital economy. His work has encompassed topics as diverse as the internet of things, online advertising and intellectual property rights.

Stacie Hoffmann is a Consultant at Oxford Information Labs. She advises industry, policy makers, regulators, and civil society around the world on the intersection of technology and policy. Her areas of expertise include cyber and information security, emerging technologies, and technical standardisation.

Mark McFadden is a Senior Associate at Oxford Information labs. Mark has more than 30 years of operational and policy experience in IP addressing, internet governance and cybersecurity Mark is an active contributor to work in the Internet Engineering Task Force (IETF) and ICANN, and is involved in the development of global internet security and addressing standards and policies.

Akhiljeet Kaur is an Analyst at Plum. She has contributed to projects relating to digital economy, telecommunications regulation, spectrum policy and telecom operator strategy. Akhil's work has included research and analysis on data economy and emerging technology trends in the ICT industry.

Sarongrat Wongsaroj is a Principal at Plum and specialises in economic research and quantitative analysis in the fixed and mobile communications industry. He has led quantitative works in projects to assess policies in the telecommunications industry and in the market for radio spectrum.

Aude Schoentgen is a Principal at Plum and Head of Paris office. She holds a PhD in Economics and has worked on international projects in the telecom and digital sectors for private, academic and development funding clients.

Grant Forsyth is a Partner at Plum. Grant brings strong commercial experience to the development and application of strategy, policy, and regulation to the internet and to telecommunications markets, having led successful in-house teams in the UK, New Zealand and globally.

Laura Wilkinson is a Consultant at Plum. Laura's work focuses on the stakeholder impact of regulation and applies economic understanding to issues and policy within the digital, telecommunications and adjacent sectors.

Appendix B About Plum

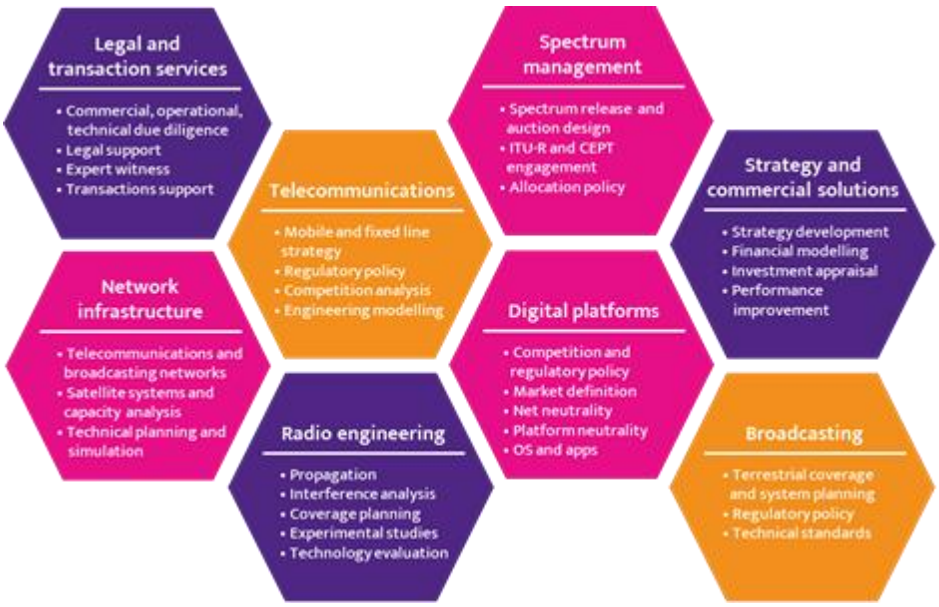
Plum Consulting is an independent consulting firm, focused on the telecommunications, media, technology, and adjacent sectors. We apply extensive industry knowledge, consulting experience, and rigorous analysis to address challenges and opportunities across regulatory, radio spectrum, economic, commercial, digital, and technology domains.

A London-based partnership founded in 2007, Plum works for governments, regulators, service providers and industry around the world. Its advice is based on rigorous economic analysis and specialist technical knowledge, which it combines with extensive market knowledge of the communications sectors to provide clear and sound analysis. Much of Plum's work is published and can be found at www.plumconsulting.co.uk

A selection of our recent work in the digital domain includes:

- A study for the Internet Society (ISOC) on the economics of the security of consumer-grade IoT products and services including recommendations to industry and policy makers to address shortcomings.
- For DCMS UK, several studies to explore online advertising in the UK, its market structure and the movement of data, content and money through the online advertising supply chain, self-regulatory initiatives and on-line harms.
- Also for DCMS, a study on the characteristics of video-sharing platforms under UK jurisdiction and their compliance with the updated Audiovisual Media Services Directive.
- Along with Oxil securing appointment on the consulting framework for the European Union Agency for Cybersecurity (ENISA), to provide it with support across its various actives to make Europe cyber secure. Economic considerations of implementing the right to data portability for a major Asian economy.

Our services



Appendix C About Oxford Information Labs

Oxford Information Labs (OXIL) is a cyber intelligence company founded in 2002 with roots in Internet policy and research. We provide consultancy and bespoke technical solutions to clients across the world including within Europe, the Americas, and the Middle East. OXIL has two streams of cyber intelligence work:

1. Policy and Big Data Analysis: We work with clients to produce world-class policy research and thought leadership on international cybersecurity issues and threats, including emerging technologies. Our technical team have proven big data analysis capabilities, and our policy team are recognised internationally for their expertise.

2. Hands-on solutions: design, implementation and delivery of cyber security solutions, Wi-Fi configuration, website protection, domain name protection, network hardening, PEN testing and red teaming, certification and training.

OXIL offers a unique blend of technical, legal and policy expertise to provide practical security solutions. Working at the intersection of policy and technology, we understand the importance, and limitations, of security's human factors and technical tools. Our experts have a wealth of experience providing tailored security solutions that work for our clients and communicating this information to a wide range of audiences.

The OXIL team provides thought leadership related to cyber security, emerging technologies and technical standards. This includes providing clients with strategic advice, evaluations and risk assessments, targeted outreach, written reports, teaching, training, research, and issue tracking across a wide range of internet governance and policy issues. Recent areas of work include 5G, DNS over HTTPS, technical standardisation, 'new IP', disinformation and elections, internet governance, social media platforms and human rights, and digital divide issues. A full list of their available publications can be viewed at https://oxil.uk/publications/.

OXIL is also well-versed in the domain name system (DNS) and Top Level Domains (TLDs). OXIL is the research team behind the long-standing EURid UNESCO World Report on Internationalised Domain Names. Every year, the team uses its technical skills to crawl the entire zone files of the gTLD space – nearly 200 million domain names. The research team has also provided the data analysis for large scale studies of the domain name marketplaces in the Middle East and Latin America (for ICANN) and for CENTR, the regional organisation for European ccTLDs.

OXIL has provided technical services and software to major internet governance companies including EURid, ICANN, CENTR, and Nominet. This includes designing and implementing the workflow system for Nominet's award-winning Dispute Resolution Service in 2001, and helping develop major components of Nominet's infrastructure services over several years. OXIL is the team behind Netistrar (an ICANN accredited registrar licensed to sell domain names).