

University of Groningen

## Global Regulations for a Digital Economy

Beaumier, Guillaume ; Kalomeni, Kevin; Campbell-Verduyn, Malcolm; Lenglet, Marc; Natile, Serena; Papin, Marielle ; Rodima-Taylor, Daivi; Silve, Arthur; Zhang, Falin

*Published in:*  
Global Policy

*DOI:*  
[10.1111/1758-5899.12823](https://doi.org/10.1111/1758-5899.12823)

**IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.**

*Document Version*  
Publisher's PDF, also known as Version of record

*Publication date:*  
2020

[Link to publication in University of Groningen/UMCG research database](#)

*Citation for published version (APA):*

Beaumier, G., Kalomeni, K., Campbell-Verduyn, M., Lenglet, M., Natile, S., Papin, M., Rodima-Taylor, D., Silve, A., & Zhang, F. (2020). Global Regulations for a Digital Economy: Between New and Old Challenges. *Global Policy*, 11(4), 515-522. <https://doi.org/10.1111/1758-5899.12823>

### Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

### Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

*Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.*

# Global Regulations for a Digital Economy: Between New and Old Challenges

Guillaume Beaumier 

*University of Warwick & Université Laval*

Kevin Kalomeni

*Luiss Guido Carli University & Université Laval*

Malcolm Campbell-Verduyn

*University of Groningen*

Marc Lenglet

*NEOMA Business School*

Serena Natile

*Brunel University London*

Marielle Papin,

*Université Laval*

Daivi Rodima-Taylor

*Boston University*

Arthur Silve

*Université Laval*

Falin Zhang

*Nankai University*

## Abstract

Digital technologies are often described as posing unique challenges for public regulators worldwide. Their fast-pace and technical nature are viewed as being incompatible with the relatively slow and territorially bounded public regulatory processes. In this paper, we argue that not all digital technologies pose the same challenges for public regulators. We more precisely maintain that the digital technologies' label can be quite misleading as it actually represents a wide variety of technical artifacts. Based on two dimensions, the level of centralization and (im)material nature, we provide a typology of digital technologies that importantly highlights how different technical artifacts affect differently local, national, regional and global distributions of power. While some empower transnational businesses, others can notably reinforce states' power. By emphasizing this, our typology contributes to ongoing discussions about the global regulation of a digital economy and helps us identify the various challenges that it might present for public regulators globally. At the same time, it allows us to reinforce previous claims that these are importantly, not all new and that they often require us to solve traditional cooperation problems.

Over the years, many have argued that digital technologies pose unique regulatory challenges for states (Fraundorfer, 2017; Herrera, 2002; Schwab, 2017). Their fundamental fast-pace and transnational nature are broadly construed to be

incompatible with the relatively slow and territorially bounded public regulatory processes. In addition, it is argued that the greater ability of private companies to conceal or move their activities in the digital realm means that

even if governments are successful in devising rules, they might not be able to implement them. These arguments are not new and were at the heart of the globalization debates at the turn of the millennium (Friedman, 2005). Then as now, assertions claiming that public regulations are an old and ill-adapted form of governance are grossly exaggerated. As shown by previous contributions (Goldsmith and Wu, 2006; Mueller, 2010), states have continuously found ways to apply their rules in the digital space. This however does not mean that crafting new and applying existing laws and regulations for the digital economy is not sometimes a daunting task.

In this paper, we argue that not all digital technologies pose the same regulatory challenges. We more precisely maintain that the *digital technologies'* label can be quite misleading as it actually represents a wide variety of technical artifacts. This clarification appears even more necessary as various policy papers increasingly present digital technologies in broad terms or talk of regulating the digital economy without clearly distinguishing the different issues raised by different technical artifacts (ICC, 2016; Kallmer, 2017; OECD, 2019). Based on two dimensions, the level of centralization and (im)material nature, we provide a typology of digital technologies that importantly highlights how different technical artifacts affect differently global distributions of power. While some can provide states with new ways to achieve their regulatory preferences globally, others can importantly limit their capacity to regulate. By emphasizing this, our typology contributes to ongoing discussions about the global regulation of a digital economy and helps us identify the various challenges that it might present for public regulators globally. At the same time, it allows us to reinforce previous claims that these are importantly not all new and that they will often require states to solve traditional cooperation problems if they want to promote the global adoption of digital technologies and ensure that their regulations remain effective. This will however be difficult to achieve as power considerations increasingly come into play and might derail all forms of cooperation.

### 1. Economic regulations in a digital world

The move from a physical to a digital economy implies that various types of physical goods and services are being progressively replaced by electronic information. From books to banking services, tangible assets are converted to digital data, which becomes one of the key assets for private companies. As illustrated by the case of Uber, owning proprietary algorithms and information on millions of users can even be more valuable than owning the physical capital required to offer a specific service. By reducing transaction costs, the use of digital technologies importantly supports the 'servicification' of the economy (Lanz and Maurer, 2015), a process by which goods are more and more consumed as services. High hopes are nowadays placed on the use of Big Data, as its proponents believe it will lead to significant efficiency and productivity gains (Mayer-Schönberger and Cukier, 2013).

In a world where so much value comes from the use of digital data, new regulatory concerns are on the rise. From privacy, to taxation and workforce transition, various issues are challenging our political systems and economies. Faced with this, public regulators worldwide are expected to ensure that digital technologies support global economic development. A cautionary note is necessary at this stage. The development of digital technologies should neither be seen as neutral nor entirely independent from the regulations created to govern them. As long recognized by the Science and Technology Studies (STS) literature, new technologies and their regulatory regimes are both influenced by the specific social and political environment in which they emerge (Bijker et al., 1989). With that in mind, public regulators can nonetheless affect the use of specific technologies at different points in time by adopting new regulations. In the context of digital technologies, this capacity of public regulators has however been argued to be limited by some of the very features of digital technologies.

For quite some time now, it has been claimed that a mismatch exists between digital technologies' global reach and geographically bounded states' legal authority (Fraundorfer, 2017; Herrera, 2002). In 2006, Brazilian authorities were for example forced to issue a subpoena to Google's headquarters in Silicon Valley to gain access to data from Brazilians. Previous requests made to Google's subsidiary in Brazil had been rejected on the basis that the data was stored on servers located in the United States (Chander, 2013). Even though Google ended up complying with the Brazilian request, it reflected its long-standing policy 'of keeping data about its users in the US to protect it from disclosure to foreign governments' (Chander, 2013). The incapacity of the US to block WikiLeaks from sharing secret documents related to the Iraq war shows that even powerful states can find it hard to deal with private actors based outside of its territory (Tusikov, 2016). Despite a massive campaign against WikiLeaks orchestrated by the American government that included cutting the organization from PayPal's payment service (Benkler, 2011), WikiLeaks in effect continues to leak sensitive information from outside the United States.

Besides the question of the territoriality of states' legal authority, the fast-paced and technical nature of digital technologies is also used to maintain that private actors *can* have a better understanding of how specific technologies function and, concomitantly, of the challenges that they pose to regulation. According to leading techno and market-evangelists, like the founder and chief executive of the World Economic Forum, the relatively slow regulatory processes of governments are simply 'unable to cope with the speed of technological change' of the digital age (Schwab, 2017, p. 69). This is in line with the long-standing (neo)liberal view that market self-regulation is generally more effective than public regulation.

Contrary to these claims, states maintain significant regulatory capacities to curtail and influence technological actors. Digital companies still have a physical presence. As shown in the above case of Google, their main headquarters are often in the US and thus fall under American

jurisdiction. While it might give them some form of legal protection, it also means that they have to respect American law. Moreover, states can also rely on other intermediaries to ensure that their rules are complied with. Payment services, like Paypal in the case of Wikileaks, as well as local telecommunication companies are two common examples (Goldsmith and Wu, 2006). Importantly, not all states however have the same leverage over these private intermediaries and different types of digital technologies will affect differently public regulators' capacity to assert their authority over them. Over the years, specific digital technologies have in fact aimed to reduce to a minimum the number of intermediaries or make them harder to identify (see below type 4). The multiplication of intermediaries can inversely question the capacity of regulators to enforce their rules. Not all states finally have the same access to the physical infrastructure of digital technologies (Denardis, 2012).

In addition to creating a number of challenges for various regulators, this has important implications for global power distributions. By increasing or limiting the capacity of action of regulators, digital technologies are in effect an important source of power for governments (McCarthy, 2015; Powers and Jablonski, 2016). As opposed to broad conceptions of power emphasizing situations where 'A has power over B', digital technologies can be seen as providing 'power to' achieve specific regulatory aims (Isaac, 1987). These can be multiple and can even lead to no action being taken by regulators. This will always depend on the ideas and interests in place. Nonetheless, by providing more easily or not access to intermediaries with a global outreach, some regulators will be more empowered than others. By having clear regulatory authority over Google and its search engine algorithm, the United States can for one more easily enforce its regulatory preferences globally. At the same time, this power to act will always remain partial if states do not cooperate with each other, and especially in cases where regulating digital technologies require to deal with many intermediaries across multiple jurisdictions (Goldsmith and Wu, 2006). While zero-sum game thinking can push regulators to act alone, their regulatory power will actually be magnified when they work together. To highlight how different technical artifacts pose different challenges to regulators worldwide and affect differently power distributions, the next section builds a typology of digital technologies. This integrated approach in turn allows us to identify where the global regulation of digital technologies will be particularly difficult and to what extent this is new.

## 2. Sorting out digital technologies

As of now, no comprehensive list of characteristics has been put forward when talking about digital technologies. Most commonly, a four layer model is used to differentiate which technical artifacts need to be regulated (Fransman, 2010). Inspired by the TCP/IP protocol stack, these models closely approximate the technical design of digital ecosystems and have in effect been good to identify potential domain of

regulation. They are moreover helpful to highlight how multiple technical artifacts build on each other to offer integrated digital services. They however fail to highlight how different technical artifacts raise different political-economic challenges for regulators. To differentiate digital technologies based on their political-economic implications, we propose a typology using two interrelated dimensions: centralization and (im)materiality. While these two dimensions are not the only ones available to classify digital technologies, they have been at the heart of the debates over the regulation of digital technologies and thus allow us to build four ideal types that are particularly meaningful to understand the challenges they can pose for public regulators.

First, centralization looks at the extent to which specific technologies support few or many intermediaries. High capital requirements and network effects are two key variables to understand why some digital technologies tend to be centralized. Despite inspiring stories behind the humble origins of many large tech companies, few digital technologies nowadays emanate from a garage or a university dorm, and if they do, they are soon bought up by the very companies (i.e., Apple, Google and Facebook) that popularized this myth. The accumulation of massive amounts of various types of capital by few digital companies clearly makes it increasingly hard for newcomers (and, even for other large companies) to challenge their dominance. To give just one example, Microsoft had to spend over \$4.5 billion to build Bing to compete with Google in the search industry. Yet Bing still holds less than 3 per cent of market share in web search globally, with more than 90 per cent of the service dominated by Google (Stucke and Grunes, 2016). Similarly, when it comes to the construction of satellites or internet cables, few companies have the financial capital and the required technical expertise. Next to these high capital requirements, many digital companies' value rises with their number of users. For example, Uber drivers have more interest in using the platform the more Uber hikers join and vice versa. These network effects are not entirely new, but they are importantly magnified by the use of digital technologies allowing private companies to reach more users than ever (Srnicsek, 2017). As opposed to traditional brick-and-mortar shops, Amazon can indeed easily reach millions of consumers. This in turn leads most producers to want to sell their products on its platform and support its domination in electronic commerce.

Yet, it is not given that digital companies will necessarily lead to greater centralization and few intermediaries to regulate. The recent development of blockchain technologies is a case in point. By aiming to remove the role of intermediary third parties, the specific goal of this new digital technology is to establish a decentralized structure for the transfer of digital value. This explicit goal notwithstanding, the extent to which it is successful in doing so is open to debate. As digital technologies evolve, their capital needs tend to grow with the need for more powerful computers and network effects will increasingly come into play. There is also increasing evidence that blockchain-based infrastructures, such as payment rails for migrant remittances, tend to

combine with and remain dependent on already existing local payment infrastructures and socio-culturally specific 'last mile' dynamics (Rodima-Taylor and Grimes, 2019). Nevertheless, the extent to which digital technologies promote (de)centralization needs to be actively considered to understand the regulatory challenges that they can present for public regulators.

The second dimension is the (im)material nature of digital technologies. As previously recognized, digital is often falsely equated with immaterial structures (Deibert, 2003; Winseck, 2017). Software, data and algorithms come to mind when thinking about the digital economy. Information and intellectual property are in effect the key assets of companies like Google and Facebook. Compared to oil companies that used to be on top of the list of most valuable companies by market capitalization, these technology firms appear to have relatively few physical capitals beyond their networks of cables that serve as pipelines for data. Yet, these physical infrastructures should not be written off so easily. The digital economy is reliant on vast networks of physical infrastructures, including satellites, submarine cables, data centres, computers and an increasingly diverse set of connected goods (i.e., phones, speakers, refrigerators, etc.). The ability to control these physical facilities and the connections between them conveys an important degree of power that is often overlooked in a focus on the immaterial nature of 'the digital'.

A word of caution is necessary at this stage. Disentangling material and (im)material artifacts is a daunting task. Google search engine can only operate by making use of various physical infrastructures. Similarly, all material structures are based on some form of immaterial capital. The construction of submarine cables is for one based on countless patents. The distinction between material and (im)material artifacts should thus never be taken to be absolute. With that said, some technical artifacts subsumed under the heading of digital technologies have a clearer material presence than others, which has important implications for their regulation. Technical artifacts with a clear material nature, like physical infrastructures and connected goods, also tend to have a clear presence in the jurisdiction where they are used and active. This in turn means that every national regulator can easily exert their legal authority over them. Going back to our previous definition of power, they have a clear legal capacity to act according to their regulatory preferences. Meanwhile, artifacts with a less clear material nature do not necessarily have a clear physical tie in all jurisdictions where they have an impact. Algorithms will have to follow the rules of the jurisdictions where they are primarily registered. Similarly, the use of personal data will have to abide by the laws where they are held. However, their relatively immaterial nature means that they can have social and economic effects in jurisdictions where the regulators will not have the same physical link to assert their legal authority.

Combined together, the level of centralization and the (im)material nature of digital technologies constitute four different ideal types as illustrated in Table 1. Each ideal type importantly represents *technical artifacts*, not specific

**Table 1.** Centralization and (im)material nature

		Centralization	
		Centralized	Decentralized
Nature	Clearly Material	Type 1 (e.g.: Submarine Cables)	Type 2 (e.g.: Smart speakers)
	Seemingly Immaterial	Type 3 (e.g.: Search engine)	Type 4 (e.g.: Bitcoin protocol)

companies such as digital giants like Google and Amazon which own technologies that fall in all four quadrants. Rather than undermining the value of our table, we believe that the possibility for a company to occupy multiple positions emphasizes the importance of not using a one-size-fits-all approach when approaching the regulation of these companies. Type 1 represents the combination of material and centralized dimensions and characterizes the major physical infrastructures behind any digital service. While it is important to note that no single country or company dominates the entire global telecommunication infrastructure, there are still a few actors that play a significant role (Winseck, 2017). Type 2 is best exemplified by connected goods, which are generally comparable and highly substitutable. Production and commercialization of these goods thus result in overall more competition than the one present in the construction of the major telecommunication networks. It includes big firms like Siemens, but also smaller ones like Sonos or Fitbit that specialize in one specific type of product (i.e., smart speakers and smart watches). Type 3 refers to digital services that mainly create value from immaterial capital (i.e., information and intellectual property) and are highly centralized like the Google Search algorithm that dominates its market. Finally, type 4 is immaterial and decentralized. It reflects digital technologies like various blockchain projects that also rely on immaterial capital but aim to distribute information and knowledge rather than to centralize it in a few hands. Having sorted digital technologies in these four groupings, the next section will highlight what this means for their global regulation.

### 3. Different regulatory challenges for different regulatory objects

Our division of digital technologies into these four types is just one manner of simplifying their highly diverse and frequently overlapping nature. In effect, all four types have their own peculiarities that are difficult to subsume under one heading. Of particular importance for public regulators aiming to harness in the public interest the digital economy is that these four ideal types of technical artifacts pose different issues for their global regulation and affect global power distribution in various ways. Following the same

order as they were previously presented, this section will highlight the specific regulatory challenges posed by digital technologies and how public regulators have tried to answer it. It will also show how national power considerations can curb international cooperation and actually limit regulators capacity to act.

First, the clear material nature of digital technologies of type 1 means that they have a clear physical presence in the jurisdiction of the countries where they are active and cannot move as readily as immaterial forms of capital. Their high level of centralization entails that there are easily identifiable intermediaries with which regulators can interact. Their regulation is moreover particularly sensitive considering the critical role they play in enabling the development of new digital services. Satellites, antennas, internet cables and data centres represent nothing less than the physical infrastructure of the digital economy. As such, type 1 technologies pose regulatory questions that are similar to the regulation of public utility companies of the 19th and 20th centuries. Public regulators primarily need to find ways to promote competition without excessively limiting investment and innovation.

The regulation of these physical infrastructures however faces another layer of complexity when taking into account the global context. As essential channels through which information flows across borders, digital technologies of type 1 are an important source of structural power for states (McCarthy, 2015; Powers and Jablonski, 2016). This creates incentives for public regulators to impose market access restrictions and support the development of national champions. In the recent case of the roll-out of the highly anticipated 5G network, the United States has for example banned the dominant Chinese company Huawei and relaxed various regulations for the largest American telecommunications operators (Seligman, 2019). This included repealing the net neutrality rules that impeded Internet operators to charge different prices to different types of information passing through their networks. In doing so, the American government hoped that it would push the private sector to make the necessary investments to develop the telecommunication network of the future and help establish the United States as the global leader in 5G technologies. In recent years, other countries have also adopted data localization laws to force private companies to build local infrastructures to process digital data and limit the global influence of large American digital companies (USTR, 2018). This regulatory strategy can, however, come at the expense of future technological development and significantly limit the growth of a global digital economy.

Second, digital technologies of type 2 increasingly denote what is referred to as the Internet of Things (IoT). These are physical objects we use in our everyday lives, like fridges, television or even simple keys, and that derive a large part of their value from intellectual property materials (data, software, algorithms, etc.) and their interconnectivity with the broader digital infrastructure. As opposed to the previously discussed large physical infrastructures, there exist multiple intermediaries that can be the target of public regulations. In effect, all firms producing and selling IoT products are

subject to the rules of all the jurisdictions where they operate. One key issue for public regulators is then to ensure that unified industry standards are developed to ensure that IoT products remain interoperable, which is not always in the interests of the largest firms (Katz and Shapiro, 1985). There are otherwise risks that some firms are left out of certain value chains and that others attempt to extract rents from consumers by impeding them from using their connected goods outside of their technical systems.

As of now, various states are attempting to set industry standards for IoT products. While all can benefit from shared standards, the gains will importantly not be equally shared and first movers stand to benefit the most by shaping the future of digital technologies' regulation (Krasner, 1991). China is notably one of the most active states at the International Telecommunications Union and the International Standard Organization to establish global standards for IoT products (Beattie, 2019). In addition to making multiple proposals for new standards, it established new technical committees and sent various experts to participate to the work of these international organizations. Fearing that this could lead to China's dominance in the digital economy, the European Union has called for an alliance with the United States to promote their standards globally (Brunsdon, 2019). This rising competition accentuates the risks of regulatory fragmentation, which could further disrupt supply chains and penalize users of digital technologies of type 2.

Third, technologies of type 3 are probably the first to come to mind when people think about digital technologies nowadays. As previously said, this category includes well-known digital services offered by companies like Uber, Airbnb, Facebook, Google, Alibaba, Tencent and Amazon that have developed services based on new data collection and processing practices. They are what is increasingly referred to as digital platforms that bring together different groups of users, for example, consumers and sellers. The centralized nature of these technologies means that just as for large physical infrastructures public regulators will find it easy to identify the firms which they wish to oversee. Yet, one key difference and regulatory challenge is that their immaterial nature also means that they will not necessarily be physically located in their jurisdiction. While states hosting the headquarters of the company behind these technologies or specific part of their activities will be able to control how they are used and applied, many will be limited by the lack of a clear physical presence of these technologies on their territory and have to look for ways to reassert their regulatory authority over them.

The use of proxies and local intermediaries is one common option to solve this issue (Goldsmith and Wu, 2006; see also Benkler, 2011). Instead of directly regulating the companies behind technologies of type 3, public regulators can in effect use their links with other companies to ensure that its rules are complied with. For example, they can request local Internet service providers to block its users' access to webpages violating its hate speech or intellectual property laws. This solution remains however imperfect and works best when the goal is to block access to its market

than making technologies of type 3 actually follow new rules. The delocalization of certain physical infrastructures, like data centres, can also limit the number of local intermediaries through which regulators can act.

The development of regulations with an extraterritorial reach is one important way to solve this. Over the years, the European Union has notably designed its data protection regulations to protect the use of personal data of European wherever it is used. This regulatory approach was particularly enhanced with the recent adoption of its General Data Protection Regulation (GDPR), which gave it more power to apply fines on foreign companies. The recent decision by French regulators to tax foreign companies that are offering digital services in France is another example of this regulatory approach. This approach can, however, spur a normative competition and a complex legal environment for firms and individuals to navigate. States from where these digital services are offered can also try to limit the use of extraterritorial regulations, leading to more interstate conflicts. The United States has for example threatened to impose new tariffs on French products, which led France to suspend its new tax plan while the OECD works on a proposal. The use of extraterritoriality remains finally limited by the fact that a clear link still needs to exist between the regulators' jurisdiction and the company behind the technologies of type 3. In a recent decision on the application of the *right to be forgotten*, the Court of Justice of the European Union (CJUE) significantly maintained that an 'operator of a search engine is not required to carry out a de-referencing on all versions of its search engine' (CJUE, 2019). In effect, it only has to do so on European versions of its websites (e.g., Google.fr), significantly limiting the effectiveness of the right to be forgotten as the information would remain referenced on its other Internet domains like Google.com. Overcoming these issues will inescapably require increasing cooperation between public regulators all over the world and the development of global rules.

Fourth, and finally, type 4 technologies are probably the most difficult to conceive and regulate. Indeed, not only do their activities have a less clear physical presence, but there are also few clear intermediaries to regulate. Blockchain technologies are one recent example of this form of digital technology, which primarily aims at 're-decentralising' digital networks (De Fillipi and Loveluck, 2016; see also Kostakis and Giotitsas, 2014). In short, blockchain technologies draw upon multiple technical innovations, including most notably encryption and time-stamping, to allow the safe transfer of value without trusted third parties (Campbell-Verduyn, 2018). This can take the form of exchange of money (e.g., Bitcoin), but also of contractual rights or other valuable information. The non-proprietary and open-source nature of the blockchain protocol actually mean that anyone can use them to process any types of economic transactions. Participants' transactions are then validated by a distributed network of computers that solve complex mathematical puzzles and saved as 'blocks of data' in public ledgers.<sup>1</sup> The security and immutability of the information results both from the impossibility to change one transaction information without changing the entire chain of blocks, which would require

immense computing power, and the fact that the data is held by all participants. In other words, no single entity could in theory change the data saved in a blockchain without the consensus of the other members of a given blockchain network.

The absence of a single validation authority, such as a bank or another financial intermediary, is one reason why public authorities are puzzled or even hostile towards blockchain technologies. In effect, a network of countless entities distributed around the world does not fall easily under their control and there are obvious risks that private actors try to circumvent their legal obligations. The relatively immaterial nature of the computer code and data behind blockchains mean that it can be hard for public regulators to assert their authority over them. Even though governments can ban the use of blockchain technologies from their territory or develop rules to govern them, these regulatory actions will be difficult to enforce as they can often fall out of their jurisdictional reach. All users can *in fine* be the intermediaries regulated, but it evidently runs the risk of being ineffective. Paradoxically, working with private intermediaries might well be the best solution to regulate digital technologies of type 4 and blockchains.

Indeed, many cryptocurrency-to-state-backed-currency exchanges now enforce identification requirements while a blockchain intelligence industry has arisen to enable police and security actors to pinpoint with increasing precision the individuals involved with cryptocurrency transactions. While private actors may play a role in regulating other digital technologies, they appear particularly essential to the regulation of technologies like blockchains and crypto-assets. In effect, actors like mining companies<sup>2</sup> or online trading platforms have become the channels through which public regulators project their legal authority. Recognizing this, the government of Canada has for example amended its Proceeds of Crime (Money Laundering) and Terrorist Financing Act in 2014 to force cryptocurrency-to-state-backed-currency exchanges to implement anti-money laundering programs and report suspicious activities to the relevant enforcement agencies. Other countries, like India and China, have on the contrary decided to limit or even ban the activities of such exchange platforms on their territories. This appears to be counterproductive as it only pushes these intermediaries towards expatriation and end up limiting their capacity to monitor and influence the future development of this new technology. That being said, working via national private intermediaries will not be enough. To ensure that these technologies remain an opportunity for positive economic transformation, greater global cooperation will once again be needed. There is otherwise the risk that some actors try to circumvent public regulators' control and develop services in more lax jurisdictions, as happened with the development of exchange platforms in Malta or Panama.

#### 4. Future risks

There are few doubts that digital technologies are transforming the structure of the economy and empowering

both new and existing transnational actors. As public regulators attempt to reassert their authority in this digital era, we argued that not all technical artifacts subsumed under the concept of digital technologies pose the same regulatory challenges. Their different level of centralization and perceived materiality importantly raise distinctive issues for public regulators. Moreover, while technical artifacts of type 1 pose very few new challenges, type 4 can be more difficult to deal with. Their decentralized and relatively limited physical presence means that regulators will often need to work together and in collaboration with new types of private intermediaries. Recognizing this, various states have adapted their regulations. National responses will however often be imperfect and might even create new problems.

More specifically, states approaching the regulation of type 1 artifacts independently can first promote a securitization of the digital economy and significantly limit its global development. As control over key physical infrastructures is increasingly seen as a source of power, there is the danger that various states try to reassert their control, through potentially hostile means, or limit their dependency towards specific technologies. Meanwhile, the regulation of artifacts of type 2 creates traditional coordination problems where states have to agree on common set of standards. Failure to do so jeopardize any attempts at promoting greater competition and interoperability. The adoption of extraterritorial regulation to control technological artifacts of type 3 could also result in a normative competition and leave many states in a particularly disadvantageous position. As discussed, even powerful jurisdictions like the European Union could be limited in their capacity to act. The peculiar nature of technical artifacts of type 4 finally means that their regulation can only be effective if global cooperation is achieved. Even states with significant administrative means will need the support of smaller states to ensure their regulations are not circumvented.

A good understanding of the different regulatory challenges posed by different digital technologies is thus necessary but on its own insufficient. Global cooperation is badly needed, and international organizations have a key role to play in promoting shared understandings. This is even more essential as no public regulators have the capacity to single-handedly solve all regulatory challenges raised by digital technologies. As particularly seen with digital technologies of type 4, even regulators from powerful states will have hard time acting alone. By making the world more interdependent, digital technologies simply require global solutions. At the same time, this contribution has attempted to make clear that by affecting the distribution of power, the regulation of digital technologies will not have any easy answer. The trade and technology disputes between the US and China clearly show how difficult it will be to achieve a global consensus on the regulation of digital technologies and the precarious state of many international institutions.

## Notes

1. New blockchain networks operated by private companies importantly do not respect this public characteristic.

2. Mining here means the activity of validating transactions on the blockchain.

## References

- Beattie, A. (2019) 'Technology: How the US, EU and China Compete to set Industry Standards', *Financial Times*. Available from: <https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271> [Accessed 23 April 2020].
- Benkler, Y. (2011) 'WikiLeaks and the Protect-IP Act: A New Public-Private Threat to the Internet Commons', *Daedalus*, 140 (4), pp. 154–64.
- Bijker, W. E., Hughes, T. P. and Pinch, T. J. (eds.) (1989) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge: MIT press.
- Brunsdon, J. (2019) 'EU urges Alliance with US to Counter Chinese Tech Dominance', *Financial Times*. Available from: <https://www.ft.com/content/aabd515e-aed5-11e9-8030-530adfa879c2> [Accessed 23 April 2020].
- Campbell-Verduyn, M. (2018) *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance*. Abingdon: Routledge.
- Chander, A. (2013) *The Electronic Silk Road*. New Haven, CT: Yale University Press.
- Court of Justice of the European Union (2019) Press Release No 112/19 [online]. Available from: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-09/cp190112en.pdf> [Accessed 23 April 2020].
- De Fillipi, P. and Loveluck, T. (2016) 'The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure', *Internet Policy Review*, 5 (4), pp. 1–32.
- Deibert, R. (2003) 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millennium*, 32 (3), pp. 501–530.
- Denardis, L. (2012) 'Hidden Levers of Internet Control', *Information, Communication and Society*, 15 (5), pp. 720–738.
- Fransman, M. (2010) *The New ICT Ecosystem: Implications for Policy and Regulation*. Cambridge: Cambridge University Press.
- Fraundorfer, M. (2017) 'Brazil's Organization of the NETmundial Meeting: Moving Forward in Global Internet Governance', *Global Governance*, 23 (3), pp. 503–21.
- Friedman, T. (2005) *The World Is Flat*. New York: Farrar, Straus and Giroux.
- Goldsmith, J. and Wu, T. (2006) *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.
- Herrera, G. L. (2002) 'The Politics of Bandwidth: International Political Implications of a Global Digital Information Network', *Review of International Studies*, 28 (1), pp. 93–122. <https://doi.org/10.1017/s0260210502000931>.
- ICC (2016) Regulatory Modernization in the Digital Economy: Developing an Enabling Policy Environment for Innovation, Competition, and Growth [online]. Available from: <https://iccwbo.org/content/uploads/sites/3/2016/06/ICC-Digital-Economy-Commission-Policy-Statement-on-Regulatory-Modernization-in-the-Digital-Economy.pdf> [Accessed 10 March 2020].
- Isaac, J. (1987) 'Beyond the Three Faces of Power: A Realist Critique', *Polity*, 20 (1), pp. 4–31.
- Kallmer, J. (2017) Dear World Leaders: Tear Down Your Digital Walls [online]. Available from: <http://www.gmfus.org/publications/dear-world-leaders-tear-down-your-digital-walls> [Accessed 10 March 2020].
- Katz, M. L. and Shapiro, C. (1985) 'Network Externalities, Competition, and Compatibility', *The American Economic Review*, 75 (3), pp. 424–40.
- Kostakis, V. and Giotsas, C. (2014) 'The (A)Political Economy of Bitcoin', *TripleC*, 12 (2), pp. 431–40.
- Krasner, S. (1991) 'Global Communications and National Power: Life on the Pareto Frontier', *World Politics*, 43 (3), pp. 336–66.
- Lanz, R. and Maurer, A. (2015) 'Services and Global Value Chains: Some Evidence on Servicification of Manufacturing and Services Networks', *WTO Staff Working Paper No. ERSD-2015-03*.

- Mayer-Schönberger, V. and Cukier, K. (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*. New York: Houghton Mifflin Harcourt.
- McCarthy, D. (2015) *Power, Information Technology, and International Relations Theory*. Basingstoke: Palgrave Macmillan.
- Mueller, M. (2010) *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.
- OECD (2019) Regulatory Effectiveness in the Era of Digitalization [online]. Available from: <https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf> [Accessed 10 March 2020].
- Powers, S. and Jablonski, M. (2016) *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago, IL: University of Illinois Press.
- Rodima-Taylor, D. and Grimes, W. (2019) 'International Remittance Rails as Infrastructures: Embeddedness, Innovation, and Financial Access in Developing Economies', *Review of International Political Economy*, 26 (5), pp. 839–862.
- Schwab, K. (2017) *The Fourth Industrial Revolution*. Danvers, MA: Crown Publishing Group.
- Seligman, L. (2019) 'America's Answer to Huawei', *Foreign Policy*. Available from: <https://foreignpolicy.com/2019/10/01/america-answer-to-huawei-pentagon-carriers-5g-race-china/> [Accessed 23 April 2020].
- Srnicek, N. (2017) *Platform Capitalism*. Malden, MA: Polity Press.
- Stucke, M. E. and Grunes, G. P. (2016) *Big Data and Competition Policy*. Oxford: Oxford University Press.
- Tusikov, N. (2016) *Chokepoints: Global Private Regulation on the Internet*. Berkeley, CA: University of California Press.
- USTR (2018) Fact Sheet: Key Barriers to Digital Trade [online]. Available from: <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/march/2018-fact-sheet-key-barriers-digital> [Accessed 10 December 2019].
- Winseck, D. (2017) 'The Geopolitical Economy of the Global Internet Infrastructure', *Journal of Information Policy*, 7 (1), pp. 228–267.

## Author Information

**Guillaume Beaumier** is a Marie Curie doctoral fellow currently completing a joint PhD program at the University of Warwick and Université Laval. His work mainly revolves around the growing complexity of global governance, international trade and the digital economy. His thesis specifically looks at the evolution of data protection rules.

**Kevin Kalomeni** is a Marie Curie doctoral fellow currently completing a joint PhD program at Luiss Guido Carli and Université Laval. His work

focuses on the political impact of technical standards in finance (crypto-assets) and international trade (regulatory cooperation).

**Malcolm Campbell-Verduyn** is an Assistant Professor of International Political Economy in the Department of International Relations and International Organization at the University of Groningen. His research combines a general focus on ideas and materiality with a specific interest in the roles of non-state actors, technologies and technical artefacts in contemporary global governance.

**Marc Lenglet** is Associate Professor in the Strategy and Entrepreneurship Department at NEOMA Business School (France). His research roots in the Social Studies of Finance tradition, with a focus on regulation and algorithmic technologies. He is the co-editor of *The Making of Finance. Perspectives from the Social Sciences* (Routledge, 2019).

**Serena Natile** is a Lecturer in Socio-Legal Studies at Brunel Law School, Brunel University London. Her recent book *The Exclusionary Politics of Digital Financial Inclusion: Mobile Money, Gendered Walls* (Routledge, 2020) examines the narratives, regulation and governance of digital financial inclusion as a development strategy for gender equality.

**Marielle Papin** is a PhD candidate at Université Laval. Her main research interests are international environmental politics, cities, networks, global climate governance, and technology governance. She is currently finishing her dissertation on the novelty of transnational municipal networks in global climate governance, using network theory and complexity approaches.

**Daivi Rodima-Taylor** is a social anthropologist and research associate at the African Studies Center of Boston University, and visiting researcher at the University of California, Irvine. She has taught anthropology and international relations and engaged in longitudinal ethnographic fieldwork in African communities. Her current research focuses on the intersection of grassroots economies and digital technology.

**Arthur Silve** is Assistant Professor at Laval University in the Economics Department. His work is in the field of political economics and focuses on issues related to development and institutions.

**Falin Zhang** is an associate professor in the Zhou Enlai School of Government, Nankai University (Tianjin, China). His principal research interests lie in international political economy (IPE) and Chinese politics, and recent studies focus on international financial power competition.