INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Mapping power and jurisdiction on the internet through the lens of government-led surveillance

Oskar Josef Gstrein
University of Groningen, Fryslân, Netherlands, o.j.gstrein@rug.nl

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1497

Abstract: Facing the fragmentation of digital space in the aftermath of the Snowden revelations, this article considers regulatory models available to avoid the balkanisation of the internet. Considering government-led surveillance in particular, available strategies are investigated to create a trustworthy and universal digital space, based on human rights principles and values. After analysis and discussion of salient aspects of two relevant proposals, it is submitted that the lack of a common understanding of concepts makes global regulation unlikely. Nevertheless, a possible alternative to universal frameworks and national regulation might be the creation of 'blocs of trust', established through international conventions.

Keywords: Internet governance, Surveillance, Jurisdiction, Human rights

Article information

Received: 26 Sep 2019 **Reviewed:** 21 Dec 2019 **Published:** 16 Sep 2020

Funding: While the writing of the manuscript was not supported by any specific project or funding, a significant portion of the underpinning research has been carried out in the MAPPING project which is part of the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 612345.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/mapping-power-and-jurisdiction-internet-through-lens-government-led-surveillance

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

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

INTRODUCTION

On 6 June 2020, seven years passed since Edward Snowden commenced his revelations on governmental misuse of surveillance capabilities (Edgar, 2017, p. 75). The impact and meaning of his actions are still subject to vivid discussion. Snowden has recently refuelled this discourse

with the publication of a memoir entitled *Permanent Record* (2019), but despite considerable echo in the press and civil society campaigns, not much seems to have changed (see e.g., Stoycheff et al., 2019, pp. 613-614). At first glance this is surprising since actors such as the United Nations and the Council of Europe have undertaken several efforts to support human rights, democracy and the rule of law in the digital age (De Hert & Papakonstantinou, 2018, pp. 526-527; Terwangne, 2014, pp. 118-119). Furthermore, the United Kingdom (UK) and South Africa admitted bulk surveillance in court (Privacy International, 2019). Observing more closely, however, Snowden's activities might unintentionally have catalysed a process which leads to more fragmentation of the digital space.

In a section entitled 'The dark side of hope' in his 2018 book on the culture of surveillance, David Lyon describes the ex-employee of a contractor of the United States National Security Agency (NSA) as a thoughtful technical expert, who believes in the potential for democratic and human development through the internet. In addition, Lyon points out that Snowden revealed some of the secret mechanisms contributing to creating a world in which the majority of humans remain poor and dependent. First and foremost, underlying Snowden's revelations is the fact that 'today's surveillance undoubtedly contributes to and facilitates this world' (Lyon, 2018, p. 143). From this perspective, it is not surprising that many societies and states choose to reduce exposure of 'their' data to a multilateral setting with complex and hard-to-control implications. Rather, they shift the focus onto immediate political and economic interests. This is probably not the reaction that Snowden and his supporters might have hoped for, since it will most likely not result in more protection for human rights in the short term. However, it is the easiest answer to a myriad of complex questions.

The motives of states vary as they engage in this process of reassurance. Some focus on strengthening internal security and stability, which typically takes the form of creating legal frameworks with the objective to facilitate access to personal data for law enforcement agencies. Concrete examples are the e-evidence package of the European Union (EU), or the United States' Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Whereas e-evidence tries to make investigations across EU member states easier by removing the requirement for review by local national authorities as 'middlemen' (Buono, 2019, pp. 307-312), the CLOUD Act enables the US administration to sign agreements with states like the UK and Australia to make cross-border data access quicker and easier (Galbraith, 2020, pp. 124-128). Both of these legal frameworks aim at circumventing the complex and time consuming mutual legal assistance procedures enshrined in traditional international mutual legal assistance treaties (MLATs) (see also Vazquez Maymir, 2020, this issue).

Other countries have started to focus increasingly on maintaining external security and national sovereignty. For example, the Russian Federation has enacted regulation to strengthen the autonomy of the Russian part of the internet (Sherwin, 2019), which follows an earlier law requiring that servers containing personal data of Russian citizens must be located on state territory (Anishchuk, 2014). If one reacts sceptically to this type of decisions, one should take into account that discussions on 'digital sovereignty' are not only taking place in seemingly 'inward looking' countries, but also seemingly in 'open-minded' ones such as Germany (Fox, 2018; Gräf et al., 2018). At the same time, the People's Republic of China seems not to distinguish between political and economic power, and pursues regulation that also limits the international exchange of economic data flows (Yang, 2019).

These observations create the impression that the interest in investing in further development of a multi-stakeholder mechanism for internet governance is limited. This mechanism gathers

states/governments, the private sector, civil society, intergovernmental organisations, international private organisations, as well as the academic and technical communities to shape the global internet through interactive discourse (Hill, 2014, p. 29). Organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF), or the International Telecommunication Union (ITU) take prominent roles in this process. They differ considerably when it comes to democratic anchorage, legitimacy, representation, as well as regulatory authority, which results in undeniable tension with institutions of traditional governance. While some national administrations fear loss of sovereignty, several groups of civil society feel under- or non-represented (Ewert et al., 2020). Hence, the decentralised and universal nature of the internet, which are both paradigms that the multi-stakeholder mechanism traditionally supports (Hill, 2014, pp. 16-46), has become subject to scrutiny. Scholars such as O'Hara and Hall argue that there are already four internets: a heavily regulated European 'bourgeois' version that prides itself on its dedication to human rights and ethics; the US version with its strong focus on monetisation and economic activity; the authoritarian internet of China where social cohesion and surveillance mean the same thing; and the internet of misinformation and hacking associated with the Russian Federation, North Korea and other 'rogue states' (O'Hara & Hall, 2018).

If anything, this makes it clear that the nature of the internet is still developing. Since John Perry Barlow published the 'Declaration of the Independence of Cyberspace' (1996) the digital sphere has evolved considerably. The internet has become an important layer of social interaction which also means it has become more than a mere passage for data flows. While the idea to regulate it in a similar way to what Hugo Grotius suggested for the High Seas in 1608 seems appealing (Hildebrandt, 2013, p. 211) - particularly to those primarily concerned about the free passage of data packages - the technical infrastructure that constitutes the internet cannot be qualified as *res nullius*. In contrast to the High Seas, the internet does not lend itself neutrally to any kind of activity. In this context, Melvin Kranzberg's first law is not the only thing that comes to mind ('technology is neither good nor bad; nor is it neutral' (Kranzberg, 1995, p. 5)). As inhabitants of industrialised and more developed countries face the looming threat of being replaced by 'superintelligent' autonomous machines (West, 2018, pp. 19-41), the rushed and under-reflected adoption of 'digital identities' might further widen the inequality gap with less-developed areas of the world (Gstrein & Kochenov, 2020). Hence, as the rapid mass-adoption of information technology and autonomous systems continues, this urgent question emerges: is it possible to create a trustworthy and universal digital space, based on human rights principles and values, which might be able to prevent a dystopian future with limited opportunities for information exchange and undignified data-driven economies whose purpose is to fuel fantasies of political hegemony?

The objective of this article is to identify potentially useful regulatory strategies that at least mitigate or avoid (further) balkanisation/fragmentation of the digital space. This process of fragmentation has also been described as movement towards a 'splinternet'. Once it is completed, the remaining digital information networks will have turned away from the three central principles of openness in terms of universal cross-border data transfer, trust in terms of faith in other users, and decentralisation which supports resilience and freedom (Ananthaswamy, 2011, p. 42). The lens through which the regulatory strategies will be identified is government-led surveillance as defined in the Methodology section. After analysis of two proposals for the regulation of government-led surveillance from a universal perspective, available strategies to manage power and jurisdiction on the internet will be discussed. At the end of this exercise it will be concluded whether regulatory frameworks that respect, protect and promote the internet as one global space are feasible under current circumstances.

METHODOLOGY

Before starting to map out salient issues, a few brief remarks on the selection of proposals and the methodology of this submission are necessary. The topic of surveillance is immensely complex with much historic context to consider (Galič et al., 2017). Additionally, surveillance as a phenomenon is not only purely government-driven. Much has been written about the profiling of individuals for commercial gain, the impact of 'surveillance capitalism' (Zuboff, 2019) on individual and collective autonomy, and how new technologies such as artificial intelligence influence democracy and the formation of the public (Nemitz, 2018). Other scholars propose the consideration of surveillance 'as cultural imaginaries and practices' which makes surveillance a subject of everyday life (Lyon, 2018, p. 127).

While these are valid approaches, this submission will predominantly leave out major corporate and non-government related aspects. For this piece the term 'surveillance' is defined as 'any monitoring or observing of persons, listening to their conversations or other activities, or any other collection of data referring to persons regardless whether this is content data or metadata'; furthermore, government-led is to be interpreted as 'surveillance [that] is carried out by a state, or on its behalf, or at its order' (Cannataci, 2018a, p. 9). These definitions emphasise the relationship between the citizen/resident and the state, which is typical for international human rights law. Furthermore, this concentration makes the topic more manageable in volume, and allows distilling the essence of available regulatory strategies. However, this does not suggest that regulation is all that is required to create a trustworthy and universal digital space. Furthermore, applying government-led surveillance as a lens with its focus on states and individuals does not mean that the actions of corporations are entirely irrelevant. As supporters or enablers of state surveillance - which has been claimed to reach structural dimensions embedded in the telecommunications infrastructure of powerful western actors (Gallagher & Moltke, 2018) - their actions remain relevant. The United Nations stressed such responsibility in a General Assembly resolution on privacy in the digital age on 14 November 2018 (2018, pp. 6-7).

In this setting focused on regulatory frameworks for government-led surveillance, the available regulatory strategies are explored on the basis of two recent proposals which attempt to address the issues on universal level: The 'Working Draft Legal Instrument on Government-led Surveillance and Privacy' ('LI') (Cannataci, 2018a) which has been presented to the United Nations Human Rights Council in March 2018, and the proposal for a 'Digital Geneva Convention' (DGC) presented by one of Microsoft's presidents Brad Smith (2017).

GENERAL NATURE OF THE PROPOSALS

Both proposals are based on the premise that the internet is an independent and universal/global space which should be accessible and open to all individuals on the planet regardless of where they come from. By emphasising this enabling and empowering dimension from an individual perspective, the proposals call on states to overhaul the international legal framework in order to address government-led surveillance in more detail and more effectively (Cannataci, 2018b, p. 22; Smith, 2017). Smith starts with the observation that cyber-attacks, cyber-espionage and cyber-warfare have become widespread and dangerous (see also Thumfart, 2020). Since many of these are directly or indirectly led by state powers that carry out

surveillance, he proposes to address this new reality with the development of a DGC to protect private citizens and entities, or in other words 'non-combatants' (Smith, 2017). His proposal relates to the Fourth Geneva Convention for the protection of civilians in warfare from 1949 (Mansell & Openshaw, 2010, p. 23). Since the appropriateness, effectiveness, and timeliness of the Geneva Conventions of 1949 is being questioned due to the emergence of asymmetric warfare and international terrorism in today's conflict scenarios (Gordon 2010, pp. 95-96; Ratner, 2008), it might be surprising to see such a concrete demand spearheaded by one of the presidents of one of the most influential technology corporations. Smith (2017) suggests enshrining six principles in a novel instrument of public international law: (1) No targeting of tech companies, private sector or critical infrastructure; (2) Assist private sector efforts to detect, contain, respond to, and recover from events; (3) Report vulnerabilities to vendors rather than to stockpile, sell or exploit them; (4) Exercise restraint in developing cyber weapons and ensure that they only allow for limited and precise use; Additionally, they should be non-reusable; (5) Commit to non-proliferation activities relating to cyberweapons; and (6) Limit offensive operation to avoid a mass event. In terms of impact, the DGC has not gained traction within the community of states at the time of writing. However, it was followed up with the signing of a 'Cybersecurity Tech Accord' by 34 technology and security companies in 2018 (Smith, 2018).

The principles of the DGC have to be evaluated critically, keeping in mind that Smith is associated with a corporation that has strong relationships with some of the most powerful states. On the one hand, this scepticism *vis-à-vis* Smith's intention was recently supported with the award of a US$ 10 billion contract by the United States Pentagon which allows Microsoft to provide an advanced cloud infrastructure for the United States Army that might also be used for surveillance (Conger et al., 2019). On the other hand, when focusing on the substance of his proposal one can also discover aspects that support openness, trust and decentralisation of the internet by making the internet less dependent on traditional governance mechanisms and institutions. Hence, the DGC is potentially able to support the creation of a digital space which is universal and safe(r) for its users. For example, the United States NSA recently shared the discovery of a major security vulnerability in Windows systems that could have facilitated large scale surveillance if kept secret (Newman, 2020). In this sense the agency delivered on the demands enshrined in principles two and three of the DGC. Furthermore, it seems fair to assume that corporations focus predominantly on the relationship with their users/clients who do not only consist of governments. Their business opportunities increase with the ability to act in stable and universal legal frameworks across the globe, independent from territorial restraints. This also means there is an interest in having checks and balances that control public institutions as they carry out surveillance, since the independence of the private sector is strengthened. This also means that aspects like citizenship or residency do not matter as much for corporations as they do for states, and in traditional human rights/civil liberties law when it comes to applicability and enforcement (Nowak, 2018, pp. 273-275).

Smith's proposal is based on a perspective where technology corporations are independent and neutral actors which promote the internet as a universally accessible layer of societal interaction. Whether this is a sincere, desirable or achievable objective can remain for speculation. Regardless, the DGC as a blueprint for a regulatory instrument in itself is a worthy object of study for the purposes of this article. While Smith and Microsoft's intentions might be more or less motivated by economic short-term gains in their day-to-day business, the DGC can be scrutinised as a self-standing set of principles that has its own strengths and weaknesses, which will be outlined below.

Although the DGC and the LI have the common goal of catalysing the evolution of international public law to achieve regulation of government-led surveillance, the process in which the LI emerged differs significantly. In its essence it is a co-production of an EU funded research project (MAPPING i.e. Managing Alternatives for Privacy, Property and Internet Governance) and the initiative of the inaugural UN Special Rapporteur on the Right to Privacy Joseph A. Cannataci (2018a, p. 3). The text itself, which is a sort-of blueprint for an international agreement between states, is based on earlier surveillance-related research carried out in other EU funded projects. Those insights were combined in a first draft with international and European human rights law principles, such as those enshrined in the International Covenant on Civil and Political Rights of the United Nations (ICCPR), the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the EU (CFEU). Furthermore, developments in the modernisation of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108; updated by protocol CETS No. 223 on 10 October 2018 to become Convention 108+) as well as the EU General Data Protection Regulation (GDPR) were included. Finally, the findings of landmark judgments of national courts, the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) were also taken into consideration.

Although international human rights law standards of the UN such as Article 12 of the Universal Declaration of Human Rights or Article 17 of the ICCPR underpin the provisions of the LI as well, one might criticise this heavy influence of European standards, regulation, and jurisprudence on a proposal that was developed to potentially become the basis for a global regulatory framework. Nevertheless, the initial idea for this project was to start with a relatively concrete and substantive text that would allow the mapping of salient issues in this area, as well as creating the ability for concrete discussions about them. Furthermore, international comparative research on the development of data protection and privacy law shows that European standards have heavily influenced regulation in those 142 states which did have specific privacy-related regulation at the end of 2019, the majority of which are located outside the EU, the territories of Council of Europe member states, and the United States. Additionally, the relevance of European activity is underlined by the fact that the number of specific laws across the world has risen significantly following the attention that the GDPR and Convention 108+ have received (Greenleaf & Cottier, 2020, pp. 24-26).

The final published version of the LI consists of 18 articles accompanied by explanatory remarks ('memorandum'). Before the LI was presented to the Human Rights Council in March 2018 it went through a process of thirteen substantive iterations which were based on feedback received in ten meetings carried out in different locations in Europe and the United States from April 2016 to February 2018, as well as written submissions and verbal feedback (Cannataci, 2018a, pp. 1, 38). This feedback was sourced from a multi-stakeholder community consisting of corporations, members of the law enforcement and intelligence community, members of civil society organisations, academics and other experts on the topic of government-led surveillance (Cannataci, 2018a, p. 2).

SALIENT ISSUES

Due to the limited amount of space in this article it is not possible to discuss the proposals in their entire breadth and depth. Furthermore, rather than considering them as detailed and sufficient solutions for the complex issue, it might be more appropriate to use them as indicators (or 'maps') which together might be capable of highlighting why it is so difficult to regulate

government-led surveillance. The proposals are probably best understood as attempts to reveal the substantive issues which should be resolved in order to establish the basis for progress. Although some may claim that it is unlikely that global consensus on these matters is achieved at all given the relevance of cultural differences across and within regions (Vecellio & Segate, 2019, pp. 83-88), it is precisely this audacious aspiration of becoming the basis for a discussion on detailed universal standards which bears the potential to highlight links, gaps and frictions.

WHAT IS (MASS-)SURVEILLANCE?

Probably the most discussed issue in the aftermath of the Snowden revelations is what government-led (mass-)surveillance is, could be, and should be (Buono & Taylor, 2017). The use of 'Big Data' to support national security, law enforcement and the public order requires adjusted and new safeguards to protect individuals and their rights (Broeders et al., 2017, pp. 311-321). The DGC principles do not explicitly provide a conceptual definition of mass-surveillance. Reading principles one, three, four, five and six together and attempting to combine their content in one statement, surveillance seems to be based on the use of cyberweapons which exploit security vulnerabilities. Furthermore, cyberweapons should not be used to target the private sector, and their use results potentially in mass events.

Article 2 paragraph 1 of the LI defines surveillance as 'any monitoring or observing of persons, listening to their conversations or other activities, or any other collection of data referring to persons regardless whether this is content data or metadata.' It goes on to add that 'surveillance is carried out by a state, or on its behalf, or at its order' (Cannataci, 2018a, p. 9). To understand this broad definition better it should be added that the LI uses a distinction between 'surveillance data' and 'non-surveillance data' which stems from the understanding that data is produced either by systems that are predominantly operated to carry out surveillance, or systems which have another primary purpose. The obligations stemming from the use of these different kinds of data differ in the LI, and it remains open whether it is always possible to make such a categorical distinction in practice. There might be cases in which repurposing historical surveillance data or reinterpretation/-combination of openly available data with confidential data are not covered by the provisions of the LI. Potentially, it is too strongly focused on the generation and initial processing of data, therefore underestimating the amount of usable information already available. In this regard, it might also be interesting to consider how the trend towards open source intelligence (OSINT) impacts the work of states when carrying out surveillance (Hassan & Hijazi 2018, pp. 341-345).

Article 3 paragraph 6 exempts the surveillance of military personnel from the scope of the LI. Hence, this is the only area in which the LI does not mandate that states create a dedicated law for the authorisation of surveillance which also comes with the obligation to install corresponding oversight institutions, safeguards, and remedies (Cannataci, 2018a, pp. 9, 11). An important consequence of this exemption is that all other surveillance activities - those carried out within a state through law enforcement agencies, those carried out externally through security and intelligence services, as well as those carried out through (private) mandated entities working in both domains - are subject to the same principles and rules according to the LI.

This very broad definition of surveillance covers many activities, which makes a clear distinction between 'targeted' and 'mass'/'bulk' surveillance potentially less relevant. Indeed, it might be more useful to focus the discussion on the concept of surveillance as such, since the emphasis of 'bulk' or 'mass' capabilities often seems to add little in substance. Ultimately, such narrowing of the focus could transform the public dialogue into a mock debate that is predominantly held to

capture attention. Especially when considering the rich case law encapsulated in the ECtHR's factsheet on 'mass surveillance' (2019), it needs instead to be decided on a case-by-case basis whether any kind of surveillance is legitimate (i.e. proportionate and necessary). The relevant substantive criteria to decide whether 'bulk surveillance' measures are compliant with human rights law also need to be as strict and coherent as for targeted surveillance measures.

SUBSTANTIVE SCOPE

While it has already been established that both proposals transcend territorial borders - which might support making progress on otherwise very complex problems relating to data localisation and differing regulatory requirements due to incompatible standards and fragmentation as highlighted in particular through the CJEU *Schrems* case (Kuner, 2017, pp. 917-918) - this feature in turn results in the requirement to define the substantive scope of the instruments more granularly. Since the kind of actions they target is less clear, it is more important to define them in principle. Smith's DGC attempts to resolve this issue by embedding the proposal in a description or narrative of a constantly ongoing hostile conflict in the digital domain, which results in a predominantly negative and almost implicit definition of the substantive scope. This comes with the consequence that one has to share the underlying assumptions and worldview of Smith before being able to substantively engage with the content.

If one were to define the substantive scope positively however, there are at least two perspectives which need to be taken into account: the individual/user perspective, and the perspective of the collective/regulatory institutions. When it comes to the user, French sociologist Frédéric Martel (2014, Épilogue) has made the valid argument that even in times of globalisation, users with different cultural backgrounds will continue to use the internet differently, depending on factors such as shared language, shared script, cultural perception, personal interest, etc. From the outset, this has nothing to do with interconnected infrastructure or technological features. Rather, it is the digital expression of Ludwig Wittgenstein's famous quote: 'The limits of my language mean the limits of my world' (1974, p. 68). In other words, one can complain about the fact that the government of the People's Republic of China puts technical restrictions in place which make it very difficult for its citizens and residents to access censored content from abroad. However, if one were to do so one also has to be consistent to only complain on behalf of those who are able to read the Latin alphabet and have a sufficient command of English, for example. It is very difficult to establish who truly feels limited in one's personal development (Wang & Mark, 2015, pp. 19-20). Certainly, limiting technical capabilities and putting policies in place that aim at restricting the interests of those who crave for accessing censored content will hamper the existence of a truly universal and global internet. Yet it remains uncertain how many users are genuinely interested in using such a network, at least for a significant amount of time, or when it seems reasonable to expect so.

Turning to the institutional/regulatory perspective the issue does not get much easier. As technology is constantly evolving, it makes a difference if the substantive scope is defined as either the 'internet' or the 'digital domain', which might for example also include digital information that is not being transferred through use of internet protocol addresses. One could think of the transfer of digital data using technologies such as Bluetooth, or Near-field Communication (NFC). In Article 1 sentence 1, the LI relates to 'surveillance through digital technology' (Cannataci, 2018a, p. 7) which means it adopts a relatively broad scope. This wording is the result of an attempt to align the substantive scope with the mandate of the SRP that is tied to the UN's work on human rights in the digital age (Cannataci, 2018a, p. 8). Still, one has to question if this substantive scope is precise enough for an instrument that attempts to be of global relevance and have a cross-cultural dimension. Another practical issue that might be

interesting to consider in the context of government-led surveillance is the question of what should happen if 'traditional surveillance' using non-digital means is combined with digital surveillance during a surveillance operation. In such situations it might even be relevant to have universal standards for both the digital and non-digital domains.

NECESSARY AND PROPORTIONATE

Even strong proponents of individual autonomy, privacy and data protection will agree that some form of government-led surveillance is necessary under limited circumstances, which typically include 'the prevention, investigation, detection or prosecution of crime [...] increasing public safety or protecting state security' as stated in Article 3 paragraph 3 LI (Cannataci, 2018a, p. 11). It is worthwhile comparing this provision with Article 8 paragraph 2 ECHR where it is stated that the right to respect for private and family life may be limited if it '[...] is necessary in a democratic society in the interests of *national security*, *public safety* or the *economic well-being* of the country, for the prevention of *disorder or crime*, for the *protection of health or morals*, or for the protection of the *rights and freedoms of others*' *(emphasis added)*. Hence, the LI contains fewer objectives that legitimise surveillance, and notably does not include the economic well-being of the state. In the LI's memorandum this is explained by stating that governments may legislate to punish corresponding criminal offences with an impact on economic well-being if such crimes are serious enough (Cannataci, 2018a, p. 14).

While this discussion on the legitimate objectives making surveillance necessary is interesting, more public attention was dedicated to the proportionality of surveillance measures in the aftermath of Edward Snowden's revelations. As one of the leading US civil society organisations the Electronic Frontier Foundation has developed 13 principles aimed at ensuring proportionality. These include judicial authority, due process, user notification, transparency, oversight, and others (Electronic Frontier Foundation, 2015). While the formulation of such general principles seems helpful, this might be one area where a much more granular understanding of the terms is needed. Although proportionality is a concept that is used often in international public law, there seems to be very little shared understanding of what it means objectively (Newton and May, 2014, pp. 28-32). The LI makes an attempt in this direction by proposing a three-step test in the preamble in paragraph 5 (general usefulness of the measure for the purpose; least invasive measure available used; proportionality *stricto sensu*, or considering what needs to be sacrificed/affected if feasible and least invasive measure is applied (Cannataci, 2018a, p. 3)).

In contrast, the proposal for a DGC only seems to touch upon this issue by requiring the targeted use of cyberweapons as well as restraint in their development (Smith, 2017). Remaining neutral on which kind of test is 'the right one' to resolve this issue, these considerations highlight that it is paramount to explore what the terms necessary and proportionate objectively/universally mean if any kind of international regulatory framework for this area should be developed. If it is impossible to reach such a detailed understanding through the establishment of clear definitions and detailed procedures, at least an institution needs to be appointed which has the authority to decide this on a case by case basis.

TRANSBORDER ACCESS TO PERSONAL DATA

Since both instruments have a universal scope it is particularly interesting to see how they address the question of transborder access to data. This issue was recently highlighted through the Microsoft Ireland case which developed after the United States government attempted to access data stored on a server located in Ireland, bypassing the use of lengthy traditional mutual legal assistance arrangements. Hence, Smith's corporation was at the centre of the issue,

although a similar case was also pending against Google at the time (Currie, 2017). Before the US Supreme Court decided the case, the situation was resolved by the US legislator with the introduction of the CLOUD Act (Daskal, 2018). Smith proposes in the DGC that technology companies remain neutral in this regard, solely focusing on the relationship with their users (Smith, 2017). Whether Microsoft and other technology corporations truly lived up to this principle during discussion of the CLOUD Act is very questionable however, since Microsoft, Google and others supported the legislation when it was discussed in the United States Congress (Brody, 2018). Furthermore, the DGC does not explicitly address the issue of cross-border access. Hence, the pledge for neutrality remains abstract and weak. In the end, the DGC is set in a landscape where government activities are omnipresent in the digital domain, and high information security standards would allow individuals to enjoy more privacy, regardless of where their data is physically located in the world.

The LI has a whole provision relating to this issue in Article 16. It is envisioned that its signatories would set up a new international institution consisting of experts from all participating states which would also monitor the implementation of the LI more generally. These experts would have the capacity to respond to cross-border demands in a swift manner and in procedures where the individuals affected would be represented by a 'Human Rights Defender' (Cannataci, 2018, pp. 32-35). While the establishment of this institution is compelling due to its completeness and potential to deliver a valid multilateral solution for the cross-border access problem, it remains highly doubtful whether states would be willing to transfer that much sovereign power to an international body whose actions would have significant implications for the success of criminal investigations, and potentially intelligence service activities. As the discussion within the EU about the e-evidence package shows, even in a structured regional cooperation bloc the establishment of such a central authority is not envisaged, and many gaps and issues remain to be resolved (Biasotti et al., 2018, pp. 375-420).

STRATEGIES FOR REGULATION

While the presented proposals are commendable in that they aim at supporting the ideal of the internet as a universal space dedicated to personal autonomy and individual development, the previous section makes clear that this requires much more detailed substantive understanding of key terms and concepts among the international community. While the LI is certainly more comprehensive and detailed than the DGC, it struggles to set a clear substantive scope, define the subject matter, and deliver solutions on the understanding of terms such as 'necessary and proportionate'. Key topics such as transborder access to personal data are addressed, but the whole document can only claim to be a modest step towards (more) international consensus. Hence, before universal regulation through institutions like the UN seems realistic, more detailed understanding and broad agreement on the substantive issues is required. To enable more progress on the UN level, De Hert and Papakonstantinou (2018, pp. 529-531) suggested creating a privacy-dedicated agency which could work in a similar way to the World Intellectual Property Organisation. However, this seems politically almost impossible to achieve under the current circumstances which have been outlined in the introduction. Furthermore, attempts of the UN to have more control over the internet have failed in the recent past. Just before the Snowden revelations the International Telecommunication Union (ITU) was used as a vessel for an attempt to replace the open multi-stakeholder mechanism with an open or closed model of traditional multilateral governance focused on states. During negotiations in the context of the 2012 World Conference on International Telecommunications this attempt was blocked by a

coalition led by western countries, mainly due to concerns that repressive regimes might gain too much control over the internet (Glen, 2014, pp. 643-652). Finally, there might also be valid factual reasons to have different standards and concepts as Martel's research highlights, with its focus on the user perspective (2014, Épilogue). Maybe the idea of a borderless internet-driven world was, and remains, an illusion, as Goldsmith and Wu (2006) already proposed more than 15 years ago, emphasising the role of governments and the many layers that enable the existence of the digital space.

Nevertheless, assuming for a moment that there could be more substantive consensus, the crucial question of effective enforcement also remains largely unanswered in the proposals. The DGC does not address this aspect in detail and mostly calls for states to refrain from certain actions, while the LI develops in Article 16 a perspective on oversight of its provisions through the establishment of a powerful international body operating in a centralised manner. How delicate such an attempt of attribution and redistribution of sovereign power can become can be studied by following the ongoing discussion on the 'rule of law' in the EU (Weiler, 2016, pp. 313-326). Furthermore, the German civil society organisation Stiftung Neue Verantwortung has recently presented recommendations to improve intelligence oversight (Vieth & Wetzling, 2019), which is another important element to guarantee individuals' rights and freedoms of individuals.

Hence, it seems that at the time of writing universal regulation of government-led surveillance is predominantly an academic (idealistic?; utopian?) endeavour. It is worthwhile to map the current landscape to potentially pave the way for progress, but due to the complexity of the issue it is unrealistic as a practical solution. States and regional political actors instead seem to prefer to use traditional assets and strategies to shape the internet and claim jurisdiction and power. Furthermore, restrictions about the use of the Android operating system for companies like Huawei (Afhüppe & Scheuer, 2019), or the struggle to establish trust in the deployment of 5G mobile networks suggest that this is not about to change in the near future (Matsumoto, 2019; see also Cartwright, 2020).

What other alternatives are there, leaving aside the re-territorialisation of the internet which threatens to fragment it? Is it possible to regulate topics such as government-led surveillance with strategies not using extraterritorial effect, or the reinforcement of physical borders? Such a third-way between universal frameworks and national regulation might be the establishment of 'blocs of trust'. One international agreement employing this strategy is Convention 108+ of the Council of Europe, another one the Budapest Convention on Cybercrime. These international treaties allow for a traditional harmonisation of national laws, while being open to non-member states of the Council by either acceding to them or implementing their principles in national regulation autonomously (Ukrow, 2018; Polakiewicz, 2019). Additionally, their provisions entail many useful and detailed principles, but are drafted in a way that avoids too much regulatory detail, respecting the sovereignty of states.

It is unclear how successful this strategy can be. Therefore, it will be particularly interesting to observe the push to establish Convention 108+ as a new global regulatory baseline for data protection, which is less demanding and detailed than the EU General Data Protection Regulation, but more concrete than the abstract provision on privacy in Article 17 of the ICCPR at the UN level. Maybe the areas of data protection and privacy can become pioneers in this regard, which could potentially inspire the regulation of surveillance as well. However, initial research on the requirements to adapt or (re-)model data protection laws finds that it will be difficult enough for Latin American and African countries to join the 47 member states of the

Council of Europe by signing up to Convention 108+. For Asian countries it will be even more difficult. South Korea and Thailand seem to have legal frameworks which are already mostly in line with the treaty (Greenleaf, 2020). However, this is only an analysis of requirements in terms of legal provisions, leaving aside the procedures and dynamics of political negotiation processes, as well as the question why and how countries should develop the political will to accede.

CONCLUSION

Developing blueprints for international instruments that might ultimately help to create a more harmonious and detailed framework for the regulation of surveillance on and through the internet is a commendable effort. However, in the absence of political will to develop overarching multilateral proposals on the matter, other strategies for regulation are needed. Hence, it seems that the only available alternative to such an unlikely, truly universal international framework is the development of regional frameworks which are open to third states for adoption through accession and ratification, or through modelling national laws after such agreements. The Council of Europe has been successful in developing such texts in the past (Gstrein, 2019, p. 89-90), but also has recently struggled to provide a productive forum for political exchange itself (Rankin, 2019). Certainly, this approach also comes with the danger that instead of falling back to the national level, the internet might become separated on a regional level. Still, if none of the multilateral options gain considerable influence and develop further, the only possible outcome is fragmentation of the digital space, which would also result in the reversal of many achievements made in recent times.

ACKNOWLEDGEMENT

The author thanks Taís F. Blauth for reviewing the manuscript.

REFERENCES

Afhüppe, S., & Scheuer, S. (2019, September 2). Huawei-Chairman wirbt für europäisches Ökosystem als Konkurrenz zu Google und Apple. *Handelsblatt*. https://www.handelsblatt.com/technik/it-internet/interview-huawei-chairman-wirbt-fuer-europaeisches-oekosystem-als-konkurrenz-zu-google-und-apple/24970238.html

Ananthaswamy, A. (2011). Age of the splinternet. *New Scientist*, *211*(2821), 42–45. https://doi.org/10.1016/S0262-4079(11)61710-7

Anishchuk, A. (2014, July 4). Russia passes law to force websites onto Russian servers. *Reuters*. https://www.reuters.com/article/us-russia-internet-bill-restrictions-idUSKBN0F91SG20140704

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. https://www.eff.org/nl/cyberspace-independence

Biasotti, M. A., Mifsud Bonnici, J. P., Cannataci, J., & Tudorica, M. (2018). The way forward: A roadmap for the European Union. In M. A. M. B. Biasotti, J. P. Cannataci, J., & F. Turchi (Eds.), *Handling and exchanging electronic evidence across Europe* (pp. 375–420). Springer. https://doi.org/10.1007/978-3-319-74872-6_18

Brody, B. (2018, February 7). Tech Giants Back U.S. Bill Governing Cross-Border Data Searches. *Bloomberg*.

Broeders, D. (2017). Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data. *Computer Law & Security Review*, *2017*(33), 309–323. https://doi.org/10.1016/j.clsr.2017.03.002

Buono, I., & Taylor, A. (2017). Mass Surveillance in the CJEU: Forging a European consensus. *Cambridge Law Journal*, *76*(2), 250–253. https://doi.org/10.1017/S0008197317000526

Buono, L. (2019). The genesis of the European Union's new proposed legal instrument(s) on e-evidence. *ERA Forum*, *19*. https://doi.org/10.1007/s12027-018-0525-4

Cannataci, J. (2018a). *Report to the Human Rights Council, A/HRC/37/62*. United Nations, Office of the High Commissioner for Human Rights. https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/37/62

Cannataci, J. (2018b). *Report to the Human Rights Council, A/HRC/37/62, Appendix 7 Working Draft Legal Instrument on Government-led Surveillance and Privacy*. United Nations, Office of the High Commissioner for Human Rights. https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf

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

Conger, K., Sanger, D. E., & Shane, S. (2019, December 9). Microsoft Wins Pentagon's $10 Billion JEDI Contract, Thwarting Amazon. *New York Times*. https://www.nytimes.com/2019/10/25/technology/dod-jedi-contract.html

Currie, R. J. (2017). Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"? *Canadian Yearbook of International Law*, *54*, 63–97. https://doi.org/10.1017/cyl.2017.7

Daskal, J. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *Stanford Law Review*, *71*. https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/

De Hert, P., & Papakonstantinou, V. (2018). Moving Beyond the Special Rapporteur on Privacy with the Establishment of a New, Specialised United Nations Agency: Addressing the Deficit in Global Cooperation for the Protection of Data Privacy. In D. J. Svantesson & D. Kloza (Eds.), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy*. Cambridge University Press.

Edgar, T. (2017). *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Brookings Institution Press.

European Court Human Rights. (2019). *Factsheet – Mass surveillance*. European Court of Human Rights. https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

Ewert, C., Kaufmann, C., & Maggetti, M. (2020). Linking democratic anchorage and regulatory authority: The case of internet regulators. *Regulation & Governance*, *14*, 184–202. https://doi.org/10.1111/rego.12188

Foundation, E. F. (2015). *13 International principles on the application of human rights in communication surveillance*.

Fox, D. (2018). Digitale Souveränität. *Datenschutz und Datensicherheit*, *2018*(5), 271.

Galbraith, J. (2020). United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data. *American Journal of International Law*, *114*(1), 124–128. https://doi.org/10.1017/ajil.2019.80

Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, *30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1

Gallagher, R., & Moltke, H. (2018, June 25). The Wiretap Rooms. *The Intercept*. https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/

Glen, C. M. (2014). Internet Governance: Territorializing Cyberspace? *Politics & Policy*, *5*(42), 635–657. https://doi.org/10.1111/polp.12093

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

Gordon, S. (2010). Civilian Protection – What's left of the norm? In S. Perrigo & J. Whitman (Eds.), *The Geneva Convention under Assault*. Pluto Press.

Gräf, E., Lahmann, H., & Otto, P. (2018). *Die Stärkung der digitalen Souveränität, Diskussionspapier May 2018 i.RightsLab* [Discussion Paper]. iRights.Lab. https://irights-lab.de/wp-content/uploads/2018/05/Themenpapier_Souveraenitaet.pdf

Greenleaf, G. (2020). How far can Convention 108+ 'globalise'?: Prospects for Asian accessions. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2020.105414

Greenleaf, G., & Cottier, B. (2020). 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business International Report*, *163*, 24–26.

Gstrein, O.J. (2019). The Council of Europe as an Actor in the Digital Age: Past Achievements, Future Perspectives. In J. Jungfleisch (Ed.), *Festschrift der Mitarbeiter*Innen und Doktorand*Innen zum 60. Geburtstag von Univ. - Prof. Dr Thomas Giegerich* (pp. 77–90). Alma Mater Velag Saarbrücken.

Gstrein, Oskar J., & Kochenov, D. (2020). Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World? *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.00010

Hassan, N., & Hijazi, R. (2018). *Open Source Intelligence Methods and Tools*. Apress.

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

Hill, R. (2014). The internet, its governance, and the multi-stakeholder model. *Info*, *16*(2), 16–46. https://doi.org/10.1108/info-05-2013-0031

Kranzberg, M. (1995). Technology and History: "Kranzberg's Laws". *Bulletin of Science, Technology & Society*, *15, 1*, 5–13. https://doi.org/10.1177/027046769501500104

Kuner, C. (2017). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, *18*(4), 881–918. https://doi.org/10.1017/S2071832200022197

Lyon, D. (2018). *The Culture of Surveillance: Watching As a Way of Life*. Polity Press.

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

Mansell, W., & Openshaw, K. (2010). The History and Status of the Geneva Conventions. In S. Perrigo & J. Whitman (Eds.), *The Geneva Convention under Assault*. Pluto Press.

Martel, K. (2014). *Smart – Enquête sur les internets*. Editions Stock.

Matsumoto, F. (2019, August 31). Huawei to cut engineers in Australia and restructure after 5G ban. *Financial Times*. https://www.ft.com/content/d88608f4-ca02-11e9-af46-b09e8bfe60c0

Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180089. https://doi.org/10.1098/rsta.2018.0089

Newman, L. H. (2020, January 14). Windows 10 Has a Security Flaw So Severe the NSA Disclosed It. *Wired*. https://www.wired.com/story/nsa-windows-10-vulnerability-disclosure/

Newton, M., & May, L. (2014). *Proportionality in International Law*. Oxford University Press.

Nowak, M. (2018). A World Court of Human Rights. In G. Oberleitner (Ed.), *International Human Rights Institutions, Tribunals, and Courts*. Springer Nature. https://doi.org/10.1007/978-981-10-5206-4_10

O'Hara, K., & Hall, W. (2018). *Four internets: The geopolitics of digital governance* (No. 206; CIGI Papers). https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf

Polakiewicz, J. (2019, February 26). *Reconciling security and fundamental rights*. Conference on Criminal Justice in Cyberspace. https://www.coe.int/en/web/dlapil/-/conference-on-criminal-justice-in-cyberspace

Privacy International. (2019, August 15). *Two states admit bulk interception practices: Why does it matter?* [Blog post]. https://privacyinternational.org/node/3164

Rankin, J. (2019, May 17). Council of Europe votes to maintain Russia's membership. *The Guardian*.

Ratner, S. (2008). Geneva Conventions. *Foreign Policy*, *165*, 26–32. https://www.jstor.org/stable/25462268

Sherwin, E. (2019, April 16). Russia's parliament votes to unplug internet from world. *Deutsche Welle*. https://www.dw.com/en/russias-parliament-votes-to-unplug-internet-from-world/a-48334411.

Smith, B. (2017). The need for a Digital Geneva Convention [Blog post]. *Microsoft on the Issues*. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv

Smith, B. (2018). 34 companies stand up for cybersecurity with a tech accord [Blog post]. *Microsoft on the Issues*. https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/

Snowden, E. (2019). *Permanent Record*. Pan Macmillan.

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2019). Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*, *21*(3), 602–619. https://doi.org/10.1177/1461444818801317

Terwange, C. (2018). The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data. *International Review of Law, Computers & Technology*, *28*(2), 118–130. https://doi.org/10.1080/13600869.2013.801588

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

U.K. Government. (2016). *Operational case for bulk powers*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf

Ukrow, J. (2018). Data protection without frontiers? On the relationship between EU GDPR and amended CoE Convention 108. *European Data Protection Law*, *2*, 239–247.

https://doi.org/10.21552/edpl/2018/2/14

United Nations. (2018). *The right to privacy in the digital age (A/C.3/73/L.49/Rev.1)*. United Nations, General Assembly.

Vazquez Maymir, S. (2020). Anchoring the need to revise cross-border access to e-evidence. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1495

Veccelio Segate, R. (2019). Fragmenting Cybersecurity Norms Through the Language(s) of Subalternity: India in 'the East' and the Global Community. *Columbia Journal of Asian Law*, *32*(2).

Vieth, K., & Wetzling, T. (2019). *Data-driven intelligence oversight. Recommendations for a System Update* [Report]. Stiftung Neue Verwantwortung. https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf

Wang, D., & Mark, G. (2015). Internet censorship in China: Examining user awareness and attitudes. *ACM Transactions on Computer-Human Interaction*, *22*(6). https://doi.org/10.1145/2818997

Weiler, J. H. H. (2016). Epilogue: Living in a Glass House. In C. Closa & D. Kochenov (Eds.), *Reinforcing Rule of Law Oversight in the European Union* (pp. 313–326). Cambridge University Press.

West, D. M. (2018). *The future of work*. Brookings Institution Press.

Wittgenstein, L. (1974). *Tractatus Logico Philosophicus* (D. F. Pears & B. F. McGuiness, Trans.). Routledge.

Yang, Y. (2019, April 21). Trade war with US delays China's rules curbing data transfers. *Financial Times*. https://on.ft.com/2UYQ6Eo

Zubhoff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, *28*(1), 10–29. https://doi.org/10.1177/1095796018819461