Global Constitutionalism (2016), 5:2, 145–172 © *Cambridge University Press, 2016*
doi:10.1017/S204538171600006X

Struggles for a global Internet constitution: protecting global communication structures against surveillance measures*

ANDREAS FISCHER-LESCANO
University of Bremen, Law Department, Universitätsallee GW1, D-28359 Bremen

Email: voelkerrecht@zerp.uni-bremen.de

Abstract: In 2014, the UN Human Rights Committee published its Concluding Observations on the United States' fourth periodic report on the progress of the implementation of the International Covenant on Civil and Political Rights (UN Doc CCPR/C/SR/3061), in which also the US surveillance practices are criticised. The Committee's insistence on the right to privacy and its exterritorial effect is an important first step, but it is not comprehensive, as by remaining within the individual rights framework the UN Human Rights Committee fails to sufficiently take into account the systemic challenges in play. Developing a constitution of the Internet would necessitate not only protecting individual fundamental rights against state interference, but protecting communicative spheres by guaranteeing institutional autonomies and subjecting all social spheres to democratic control; this also requires opening up spaces for a critical public, including whistleblowers, and establishing a right to cryptography – a crucial refraction in the polycentric panoptic schema.

Keywords: encryption; institutional human rights; surveillance; systems theory; whistleblowing

In its Concluding Observations on the United States' report on the progress of the implementation of the International Covenant on Civil and Political Rights (UN Doc CCPR/C/SR/3061) (ICCPR), the UN Human Rights Committee addressed among other matters fundamental and human rights issues in respect to the right to privacy that have sparked worldwide debates, known as the National Security Agency (NSA) affair. Its brief comments point in the right direction, but they disregard crucial aspects in the struggle over constitutionalising the Internet in the era of global surveillance.

The global surveillance machinery establishes a polycentric transnational panopticon, whose self-governance architecture can – building on Foucault – only be overcome by putting in place refractions and vision breaks, to prevent

* Translation into English by Nora Markard.

the apparatuses from sniffling out the remotest social corners. A systems theoretical perspective expands the Foucauldian vision, taking into account a multiplicity of threats to societal autonomies that emerge not only from the political system, but also from other societal systems. In this perspective, the global panopticon is an expression of societal polycentricity in a world society fragmented into different functional systems, each pursuing its own systemic logic.[1] Against this background, the core issues in the struggles for a global Internet constitution cast a different light on the way in which classic liberal doctrine has traditionally posited itself. The constitutional task in the transnational constellation is to release social energies in various communicative spheres and – at the same time – prevent those energies from harming human and social autonomies. The dramatic consequences of this challenge is brought to the surface in the struggles for a global Internet constitution.

I. Global surveillance

With the revelations he made in the summer of 2013, Edward Snowden drew the world public's attention to the degree to which the global networks of surveillance apparatuses control our lives. There isn't a text message, call, Facebook chat, or Google search request, a credit card operation or an email that couldn't at least potentially be downloaded, saved, scanned and fed into a network of metadata for further analysis. This is staggering in scope as approximately 194 million text message metadata run through global data bunkers every single day. Tapping into the optical fibre cables between Europe and the Far East, the NSA scans somewhere between three and six petabyte of data per day, which corresponds to the data volume of one and a half to three billion digitalised songs. These data undergo a selection process and are then stored in databases, including in the US.[2] What we call 'the cloud' may in fact be nothing more than a euphemism for a dark bunker in Idaho.

[1] Systems theory, as developed by Niklas Luhmann, assumes that world society is irrevocably differentiated into functional systems, such as the political system, the economic system, the religious system, etc. Each follows its own functional logic, seeking to maximise the interests it promotes. Humans and nature form the environment of this society of systems. See N Luhmann, *Introduction to Systems Theory* (Cambridge and Malden, MA, Polity Press, 2013). For an overview of the author's critical theory approach to systems theory, see A Fischer-Lescano, 'Critical Systems Theory' (2012) 38 *Philosophy and Social Criticism* 3–23; A Fischer-Lescano, 'A "just and non-violent force"? Critique of Law in World Society' (2015) 26 *Law & Critique* 267–80.

[2] G Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Macmillan, New York, NY, 2014) 90ff.

Panopticism

Edward Snowden's revelations have provided critical insight into a gigantic transnational panopticon.[3] Alluding to the hundred-eyed Panóptes of the Greek mythology, *panopticon* is a term that refers to a system of complete surveillance. Already in the eighteenth century, in his book *Panopticon or The Inspection House*, the utilitarian philosopher Jeremy Bentham suggested surveillance as governance technique. The panopticon, he argued, was the ideal form of organisation for prisons, factories, poor houses, hospitals, schools, etc, since it increased performance and nipped opposition in the bud early by permanent, equal, universal and all inclusive surveillance: 'Ideal perfection, if that were the object, would require that each person should actually be in that predicament, during every instant of time.'[4]

What Jeremy Bentham conceptualised as cost–benefit optimisation, Michel Foucault took as point of departure for a searing critique of society. Foucault shows how the panoptic principle pervades social conditions in all of their ramifications. In *Discipline and Punish*, he describes panopticism as the governance technique of modern societies. His criticism is directed at the resulting loss of liberty: 'Whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behaviour must be imposed, the panoptic schema may be used.'[5] But even more revealing was Foucault's analysis on the subtle effect of the casual coercion of surveillance. Security dispositives do not rely on physical coercion. They optimise powerful knowledge techniques. Interrogation management, psychiatric surveys, moralising campaigns and social work replace corporal punishment, but ultimately they affect the body more intensely. Surveillance stimulates a self-technology, which operates not externally but by initiating an observer-observation. The individuals observe themselves through the eyes of the observer. As a result, the panoptic scheme operates by way of self-discipline: 'He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own

[3] See, e.g., L Backer, 'Global Panopticism: States, Corporations, and the Governance Effects of Monitoring Regimes' (2008) 15 *Indiana Journal of Global Legal Studies* 101; K-M Simonsen, 'Global Panopticism: On the Eye of Power in Modern Surveillance Society and Post-Orwellian Self-Surveillance and Sousveillance-Strategies in Modern Art' in L Dahlberg (ed), *Visualizing Law and Authority. Essays on Legal Aesthetics* (De Gruyter, Berlin, 2012) 232.

[4] J Bentham, 'Panopticon, or 'The Inspection-House' [1787] in M Božovič (ed), *The Panopticon Writings* (Verso, London and New York, NY, 1995) 31, Letter I.

[5] M Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage Books, New York, NY, 1979) 205.

subjection.'[6] To break this pattern, it is not enough to capture the control centre. Simply occupying the tower of the panopticon does not mean stepping outside of the schema of hegemony and counter-hegemony. The goal, as Foucault puts it in his essay 'The Eye of Power', must be to rob the tower guards of their vision, to create refractions, to alter the architecture, depriving the panoptic dispositive of its premises.[7]

Transnational surveillance apparatuses

Both Bentham and Foucault start from the political dimension of surveillance and the effect it has on the subject. However, in a functionally differentiated world society, the panoptic schema operates in a much more complex manner.

Polycentric surveillance. Panopticism isn't limited to individual institutions with a top, a centre and a surveillance tower. Rather, the panoptic schema operates without limits; it is organised polycentrically. Transnational networks of surveillance apparatuses surveil even the remotest corners of society. World society is a surveillance society. It may be 'without an apex or center'[8] but the polycentric surveillance networks are no less effective than centralised panoptic institutions.

Who is behind these surveillance apparatuses? The analysis of the NSA complex revealed a whole network of secret services. Thus, the so-called 'Five Eyes' cooperate under the United Kingdom – United States of America Agreement (UKUSA Agreement), that is, the secret services of five English-speaking countries: the US National Security Agency, the British Government Communications Headquarter (GCHQ), the Australian Signals Directorate (ASD), the Canadian Communications Security Establishment (CCSE) and the New-Zealand Government Communications Security Bureau (GCSB). These work with further national secret services, including the German Federal Intelligence Service (*Bundesnachrichtendienst*, BND).

[6] Ibid 202–3.

[7] M Foucault, 'The Eye of Power', *Semiotext(e)'s Schizo-culture issue* III (1978) 2, 6–19. Asked whether those subjected to surveillance should usurp the central tower, Foucault answered: 'Yes, provided that this is not the end of the operation. Do you believe that things would be much better if the inmates seized control of the panopticon and occupied the tower, rather than the guards?' Ibid, 19 (trans. Mark Seem).

[8] N Luhmann, *Political Theory in the Welfare State* (De Gruyter, Berlin, 1990) (trans. J Bednarz, Jr, orig. 1981) 31, emphases omitted; on the polycentric Internet governance see S Taekema, 'Crossroads in New Media, Identity and Law. Fragments and Continuities of Law and ICT: A Pragmatist Approach to Understanding Legal Pluralism' in W de Been, P Arora, M Hildebrandt (eds), *Crossroads in New Media Identity and Law: The Shape of Diversity to Come* (Palgrave Macmillan, New York, NY, 2015) 80.

These state services not only cooperate with one another but also work in close coordination with international organisations such as NATO as well as private actors. In the US, in addition to the 30,000 NSA staff, 60,000 employees work for external service providers of the NSA. At the time when he collected the NSA documents, Edward Snowden himself was not directly employed by the NSA, but worked for the PC company Dell, later for the NSA service provider Booz. On top of these subcontractors involved in the surveillance network, other global players including Facebook, Yahoo, Google, Microsoft and other transnational companies collaborate closely with state security organs[9]

> One of the most significant changes that the age of surveillance has brought about is the increasing difficulty of separating surveillance by governments from that by commercial entities. Public- and private-sector surveillance are intertwined – they use the same technologies and techniques, they operate through a variety of public/private partnerships, and their digital fruits can easily cross the public/private divide […] Even if we are primarily worried about state surveillance, perhaps because we fear the state's powers of criminal enforcement, our solutions to the problem of surveillance can no longer be confined to regulation of government actors. Any solutions to the problem of surveillance must thus take into account private surveillance as well as public.[10]

Functional differentiation in world society. Finally, non-state actors are involved in surveillance not only through public–private partnerships but through functional areas, with each actor operating within them contributing to transnational panopticism. By collecting sensitive data, they pursue interests, specific to the respective functional system.

At the global economy level it is not security but the maximisation of consumption that is the key objective of the myriad international players. Data is a commodity and collecting it is a business model. At the various levels of the supply chain of the information and communications infrastructure, corporations such as Google, Apple and Facebook have virtually unlimited access to data and to the processes and content of communication within their area of authority. Applying different business models, they collect and analyse these data so as to sell them on to others for further use.[11] To optimise

[9] See also CJEU, judgment of 6 October 2015, Case C-362/14 – *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, clarifying the responsibilities of EU organs to protect against surveillance practices in the context of Facebook communication.

[10] NM Richards, 'The Dangers of Surveillance' (2013) 126 *Harvard Law Review* 1934, 1958.

[11] W Hoffmann-Riem, 'Freiheitsschutz in den globalen Kommunikationsinfrastrukturen' (2014) 69 *Juristenzeitung* 53, 53.

these business models, corporations develop their own spy software.[12] Academia, too, happily accesses the digital communication sphere to conduct research on data and surfing behaviour without obtaining user consent.[13] Other 'functional systems' contribute to transnational panopticism according to their own, specific logic. The religious system controls 'res sacrae' and believers via the Internet;[14] the health system surveys patients and promotes the health logic with Internet-based informational systems, and so forth.[15] The aim of these functional systems is clear – to regulate, and in some instances to control, the behaviour of users and followers.

In short, the functional systems of world society seek to put the worldwide web at their service, each according to their own particular interest. Surveillance and big data seeks to pursue a logic that is greater than that of securitisation.[16] Religious purification and the maximisation of profit and knowledge evoke threats as well. However, these do not result from 'old governments or industries that hate openness', but from industries and societal institutions 'that oppose those old control freaks the most'.[17]

Transformation of subjectivity

This functional differentiation of world society also transforms the understanding of subjectivity. Social discipline through subject discipline is only one manifestation of the panoptic schema. That schema is not – as Foucault conceived it – limited to involving political or legal subjects in a circle of observer-observation. The economy is not interested in potential terrorists, but in consumers; academia is interested in users as test subjects, religion in believers, health in patients, art in the *homo aestheticus*, etc.[18]

Therefore, societal autonomies are not only threatened by the totalising tendencies of the political system to limit the liberties of its subjects but

[12] A Müller-Maguhn, L Poitras, M Rosenbach, M Sontheimer and C Grothoff, 'Treasure Map: The NSA Breach of Telekom and Other German Firms' *Spiegel Online International*, 14 September 2014.

[13] R Booth, 'Facebook Reveals News Feed Experiment to Control Emotions', *The Guardian*, 30 June 2014.

[14] See, with further references, R Lewis, *God Is Watching, and So Am I: The Theology of Surveillance*, 27 April 2012, available at <http://flowtv.org/2012/04/god-is-watching>, accessed 2 February 2016.

[15] L Ohno-Machado, 'Health surveillance using the internet and other sources of information' 3 (2013) *Journal of the American Medical Informatics Association* 403.

[16] On this concept, see B Buzan, O Wæver and J de Wilde, *Security: A New Framework for Analysis* (Lynne Rienner, Boulder, CO and London, 1998).

[17] J Lanier, *Who Owns the Future?* (2nd edn, Simon & Schuster, New York, NY, 2014) 198.

[18] BC Han levels this polycentricity when he sees the 'biopolitical disciplinary society' replaced by the 'psycho-political transparency society'; BC Han, *Im Schwarm: Ansichten des Digitalen* (Matthes & Seitz Berlin, 2013) 98.

rather, functionally differentiated world society delineates boundaries within which individuals interact with the systems. It is in these parameters that threats arise from the specific energies of the specific functional systems. It is in these systemic relations within society, and in the relations of each social system to its environment, that the central problems of differentiated world society develop.[19]

II. Internet surveillance before the UN Human Rights Committee

Against this background, how does law access this polycentric panoptic schema? Which normative, and this means counterfactual, expectations is the transnational facticity of surveillance confronted with?

Legal basis and procedure of the Committee

Law is engaged with surveillance measures in contending fragments of order. Both domestic proceedings, such as in US courts under the Foreign Intelligence Surveillance Act (FISA), and supranational norms[20] and proceedings, as in the case of Google Spain,[21] have attempted to address protection against panoptic governance technology. The UN Human Rights Committee's Concluding Observations of 26 March 2014[22] is the first commentary from a quasi-judicial panel at the global level.[23]

The Committee operates on the basis of the International Covenant on Civil and Political Rights (ICCPR).[24] The Covenant was concluded in New York on 16 December 1966 and entered into force on 23 March 1976.

[19] N Luhmann, *Gesellschaftsstruktur und Semantik*, vol 2 (Suhrkamp, Frankfurt, 1993) 80.

[20] See the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) which shall enter into force in 2018 see European Council, Press Release 18.12.2015, 'EU data protection reform: Council confirms agreement with the European Parliament', available at <http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-data-protection/>, accessed 2 February 2016.

[21] CJEU, judgment of 13 May 2014, Case C-131/12 – *Google Spain*, ECLI: EU:C:2014:317.

[22] CCPR, Concluding Observations on the Fourth State Report of the United States of America, 110th Meeting, 26 March 2014, UN Doc CCPR/C/SR/3061, para 22. The state report dates from 30 December 2011. Along with the Government's response from 3 July 2013 to the Committee's list of questions, including on the NSA complex, the report is available from the US Department of State at <http://www.state.gov/j/drl/rls/c16069.htm>, accessed 2 February 2016.

[23] From the political sphere, see also UN General Assembly Resolution 68/167, *The Right to Privacy in the Digital Age*, 18 October 2013, UN Doc A/RES/68/167; see also the Report of the Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 30 June 2014, UN Doc A/HRC/27/37.

[24] 999 UNTS 171.

It has 168 state parties; a further seven states (including Cuba and China) have signed but not ratified the Covenant. The US signed the Covenant on 5 October 1977, but the ratification took another 15 years. Since 8 June 1992, the US has been bound by the Covenant, which protects the right to privacy in its Article 17.

The Human Rights Committee (or CCPR) is the UN body charged with enforcing the Covenant. An individual complaint procedure can be commenced if the defendant state has ratified the First Optional Protocol to the Covenant, which entered into force on the same date. Since the US has not accepted this procedure, matters pertaining to its obligations under the ICCPR can only be brought before the Committee in the procedures provided for in the Covenant. The US has subjected itself to the state complaint procedure under Article 41 ICCPR, but this procedure has not been used once in the history of the Covenant. Thus, when pronouncing itself on the NSA affair, the Committee was acting not under a complaints procedure, but on the occasion of the state reporting procedure under Article 40 ICCPR. This procedure obliges state parties to regularly report on the progress made in respect to the enjoyment of rights as enshrined in the Covenant. In accordance with Article 40(4) ICCPR, the Committee studies these reports from which it formulates observations.

This procedure has the potential to promote transparency where it can function as a channel for civil society efforts to keep governments in check.[25] The official state reports are regularly accompanied by so-called 'shadow reports' from NGOs.[26] The Committee also consults with NGO representatives and uses their reports as a basis for subsequent in-depth discussions with the state party.

Unlike the complaints procedures, the reporting procedure does not result in a binding decision, but in 'recommendations'. It is organised in a trial-like manner in that there is a hearing, followed by a final pronunciation that applies abstract legal norms to concrete societal facts. However, in contrast to an adversarial trail the reporting procedure doesn't seek to adjudicate an individual case. Instead, the proceedings are open, the agenda evolves over the course of the procedure and there are several opportunities for NGO representatives to make interventions. Finally, the Concluding

[25] A Liese, 'Epistula (non) erubescit. Das Staatenberichtsverfahren als Instrument internationaler Rechtsdurchsetzung' (2006) 81(1) *Die Friedens-Warte. Journal for International Politics and Organization* 51–9.

[26] Shadow Reports on the Fourth State Report of the United States can be found at the Center for Constitutional Rights, CCR (<http://www.ccrjustice.org/iccpr>, accessed 2 February 2016) or the American Civil Liberties Union, ACLU (<https://www.aclu.org/human-rights/faq-covenant-civil-political-rights-iccpr>, accessed 2 February 2016).

Observations do not set out binding legal obligations which emanate from a formal authority; their effectiveness depends first and foremost on whether the recommendations are accepted by society through the power of normative persuasion – which in turn mobilises the support of the wider public.[27]

Walter Benjamin described the forms and virtues of the intercourse between state diplomats as delicate and peaceful, because it leads to nonviolent agreement beyond legal decision-making, 'and therefore beyond violence'.[28] Similarly, the reporting procedure institutionalises forms and virtues of law that do not follow the traditional pattern of adversarial legalism, and are therefore also not characterised by the violent decision of a case. In this procedure, the methodology applied is the argumentative engagement with societal questions of responsibility. The reporting procedure is not characterised by authoritative decision-making of hard law, but by normative persuasion through argument, convincing positionality, participatory practice, responsive modes of operation, a sure sense of justice and an intuition for conflict.[29] However, under the current circumstances, this strength of the reporting procedure is also its weakness; it is often selective in the matters that it chooses to address and does not always offer an effective counterweight to the coercive apparatuses. For the problem of law and violence is profound; in a society marked by power-driven structures and conflicting interests, a procedure that forgoes legal enforcement structures risks rendering itself ineffective if it cannot counter the violence of other societal forces.

At the same time, where institutions renounce formal enforcement powers, the greatest threat arises from the political opportunism of the institution itself; a jurisprudence that panders to the interests of the states puts the legitimacy of the reporting procedure at risk. Therefore, it is rather misguided to contend that the legitimacy of forums of international justice is wholly dependent on the acceptance of the states. Indeed, global legal

[27] For a sceptical view, see S Schmahl, 'Effektiver Rechtsschutz gegen Überwachungsmaßnahmen ausländischer Geheimdienste?' (2014) 69 *Juristenzeitung* 220, 222.

[28] W Benjamin, 'Critique of Violence' (1920/21) in P Demetz (ed), *Reflections. Essays, Aphorisms, Autobiographical Writings* translated by E Jephcott (Schocken Books, New York, NY, 1986) 277, 293.

[29] For suggestions on optimising this, see U Davy, 'Welche rechtlichen Grundregeln müssen für einen wirksamen Menschenrechtsschutz gelten? Eine rechtswissenschaftliche Betrachtung' in C Gusy (ed), *Grundrechtsmonitoring: Chancen und Grenzen außergerichtlichen Menschenrechtsschutzes* (Nomos, Baden-Baden, 2011) 238, 257–8, who rightly opposes the 'master narrative' of the superiority of judicial versus reporting procedures. In particular, expanding the duty to consider the jurisprudence of the monitoring bodies could increase the position of the bodies in domestic law – see L Viellechner, 'Responsive Legal Pluralism: The Emergence of Transnational Conflicts Law' (2015) 6 *Transnational Legal Theory* 312–32.

institutions require legitimacy with respect to the 'peoples' and 'citizens'.[30] Transnational judicial forums cannot be limited to serving the needs of states, current court clients, nor can legitimacy be achieved if they do not enable those who are not included in the classic patterns of representation to be heard: the 'unrepresented' described by Jacques Derrida, the 'excluded', to quote Niklas Luhmann, the 'superfluous', as Susan Marks calls them, the 'rural poor' in Gayatri Spivak words, the 'subaltern', as Boaventura de Sousa Santos and César Rodríguez-Garavito write.[31] Transnational judicial forums will only find societal acceptance if they move beyond concentrating on procedural framing and start to critically engage with the myriad complexity of societal structural conflicts that are being translated into the *quaestio iuris*.

Applicability of the International Covenant on Civil and Political Rights

What stance, then, did the UN Human Rights Committee take on the panoptic schema? Any action by the Committee in the transnational surveillance case at hand presupposes that the Covenant is applicable in the first place.

Extraterritorial applicability: Article 2 ICCPR. First, the extraterritoriality of the measures may constitute an obstacle to the applicability of the ICCPR. The interference of surveillance measures habitually takes place beyond the territory of the surveying state, across and between boundaries. Pursuant to Article 2(1) ICCPR, a State party must grant the rights of the Covenant 'to all individuals within its territory and subject to its jurisdiction'. These two criteria apply alternatively, not cumulatively.[32]

[30] In this sense A von Bogdandy and I Venzke, 'In Whose Name? An Investigation of International Courts' Public Authority and Its Democratic Justification' (2012) 23 *European Journal of International Law* 1, 7–41.

[31] J Derrida, 'On Cosmopolitanism' in *On Cosmopolitanism and Forgiveness* (Routledge, London and New York, NY, 2001); N Luhmann, 'Inklusion und Exklusion' in Luhmann, *Soziologische Aufklärung*, 6: *Die Soziologie und der Mensch* (VS Verlag, Wiesbaden, 1995) 237; S Marks, 'Law and the Production of Superfluity' (2011) 2(1) *Transnational Legal Theory* 1; GC Spivak, 'Righting Wrongs' (2004) (2/3) 103 *The South Atlantic Quarterly* 523; B de Sousa Santos and C Rodríguez-Garavito, 'Law, Politics and the Subaltern in Counter-Hegemonic Globalisation' in de Sousa Santos and Rodríguez-Garavito (eds), *Law and Globalization from Below. Towards a Cosmopolitan Legality* (Cambridge University Press, Cambridge, 2005) 1.

[32] S Joseph and M Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, and Commentary* (3rd edn, Oxford University Press, Oxford, 2013) para 4.11ff.

The exercise of jurisdiction over an individual makes the Covenant applicable even if she is not present in the territory of the State party.[33]

There has long been debate over the definition and scope of jurisdiction; however, there is little jurisprudence from the Committee on what constitutes the exercise of 'effective control'. Indeed, already over a decade ago, the Committee, in its General Comment No 31 of 29 March 2004, asked whether the individual in question is 'within the power of effective control' of the respective state.[34] However, the European Court of Human Rights (ECtHR) expounded upon the concept of effective control in its *Al-Skeini* judgment on the extraterritorial applicability of the European Convention on Human Rights (ECHR) which serves as guidance for Article 2(1) ICCPR. The ECtHR distinguishes three forms of 'effective control', namely (1) the exercise of physical force that can bring persons under the state's control extraterritorially; (2) individualised exercise of jurisdiction by state organs abroad; and (3) domestic acts of state with extraterritorial effects.[35] Following this elaboration, surveillance measures do not necessarily amount to physical control over a person but instead to virtual control, which, due to its disciplinary effect mentioned above, can be considered equivalent to physical control with respect to the scope of application of the Covenant.[36]

Consequently, in its Concluding Observations on the United States' report, the UN Human Rights Committee determined against the continuing opposition of the US[37] that the ICCPR also applies to the US' surveillance measures – both with respect to measures within and outside of the US. It also clarified that the Covenant applies irrespective of the nationality and place of domicile of the persons concerned.[38] Affirming the extraterritorial applicability of the Covenant with respect to the surveillance measures,

[33] On the extraterritorial applicability of human rights generally, see ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 9 July 2004, ICJ Rep 2004, 136, at para 107ff; on the ICCPR specifically, see, e.g., CCPR, *Lopez Burgos v Uruguay*, 29 July 1981, Case No 52/1979, UN Doc A/36/40, paras 12.2–3.

[34] CCPR, General Comment No 31, 29 March 2004, UN Doc CCPR/C/21/Rev.1/Add.13, para 10.

[35] ECtHR, judgment of 7 July 2011, *Al-Skeini v United Kingdom*, App No 55 721/07, [2011] ECHR 1093, para 133ff.

[36] A Peters, 'Surveillance without Borders: The Unlawfulness of the NSA Panopticon, Part 2, 4 November 2013, available at <http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/>, accessed 2 February 2016, but see S Talmon, 'Der Begriff der "Hoheitsgewalt" in Zeiten der Überwachung des Internet- und Telekommunikationsverkehrs durch ausländische Nachrichtendienste' (2014) 69 *Juristenzeitung* 783–7.

[37] The Permanent Mission of the United States of America to the Office of the United Nations, Follow-up Response to the Recommendations of the Human Rights Committee, 31 March 2015, No 038-15, para 33.

[38] CCPR, Concluding Observations on the US, see (n 22) para 22.

this jurisprudence thus constitutes a first step to overcoming the legal territorial dilemma.[39] Since then, it has been supported by a number of statements in the course of the Universal Periodic Review Procedure of the Human Rights Council in May 2015. In response to the US report,[40] states and stakeholders have submitted substantial recommendations, a lot of which invoke the extraterritorial dimension of the right to privacy.[41]

No public emergency: Article 4 ICCPR. The US routinely justifies the surveillance measures with security requirements that, it argues, after 9/11 have deeply transformed the 'balance between security and civil liberties'.[42] Article 4(1) ICCPR provides for the possibility of suspending specific rights 'in time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed'. It is thus conceivable that the

[39] Concerning the exterritorial application of human rights obligations in cases of mass surveillance see also United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' see (n 23) para 31ff; Council of Europe Commissioner of Human Rights, 'The Rule of Law in the Internet and in the Wider Digital World', Issue Paper by D Korff, December 2014, 48ff; Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs, Report: 'Mass Surveillance', Rapporteur P Omtzigt, 18 March 2015, Doc 13734, 29ff; insisting on the physical effect of surveillance and on the exterritorial dimension of human rights obligations M Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56(1) *Harvard International Law Journal* 81.

[40] United States of America, National report submitted in accordance with para 5 of the annex to Human Rights Council resolution 16/21, 13 February 2015, A/HRC/WG.6/22/USA/1.

[41] See among others the critical statements on the US practice concerning mass surveillance by Azerbaijan (para 293), Costa Rica (para 294), Kenya (295), Liechtenstein (296), Germany (303) and Turkey (307) in Human Rights Council, 'Report of the Working Group on the Universal Periodic Review – United States of America, 20 July 2015, A/HRC/30/12; see also the summary prepared by the Office of the United Nations High Commissioner for Human Rights in accordance with para 15(c) of the annex to Human Rights Council resolution 5/1 and para 5 of the annex to Council resolution 16/21. United States of America, A/HRC/WG.6/22/USA/3, 16 February 2015, para 58: 'JS36 indicated that the US Government has been secretly sweeping up digital communications and personal data around the world with little oversight from either the judiciary or legislature, and recommended that the US respect the privacy of individuals outside its territorial borders. HRW made a similar recommendation. JS15 stated that the US authorities, on a daily basis, are intercepting the private communications and other personal electronic data of hundreds of millions people across the globe. JS15 recommended that the US discontinue all indiscriminate interception, retention, use and dissemination of individuals' private communications both within and outside US territory and jurisdiction.'; cf the stereotype answer of the US: 'We support these recommendations insofar as they recommend respect for ICCPR Article 17, which applies to individuals within a state's territory and subject to its jurisdiction' (Report of the Working Group on the Universal Periodic Review, United States of America, 'Views on conclusions and/or recommendations, voluntary commitments and replies presented by the State under review', 14 September 2015, A/HRC/30/12/Add.1, para 14).

[42] See the response of the US Government to the CCPR's list of questions, at (n 22) para 119; generally on the security argument, see already ECtHR, judgment of 6 September 1978, App No 5029/71 – *Klass and ors. v Germany*, [1978] ECHR 4.

US could employ the securitisation argument in a legal manner to suspend the right to privacy generally. Since the right to privacy, protected by Article 17 ICCPR, is not among the non-derogable rights contained in Article 4(2) ICCPR, such a suspension in situations of emergency is permissible.

However, the threshold for a public emergency is high.[43] Not every measure can be justified through a public emergency premise, and not every catastrophe constitutes a public emergency. Even in armed conflict, the possibility of relying on the pronouncement of a public emergency is limited.[44] Indeed, at best, surveillance measures may constitute acts of hazard control; they do not conform to the Committee's strict criteria for the existence of a public emergency. The security argument can therefore not dispense the US from the binding force of the Covenant provisions. Consequently, the US has not even moved towards taking procedural steps to declare a public emergency, which namely requires the issuing an official proclamation (Article 4(1) ICCPR) and notifying other State parties (Article 4(3) ICCPR).

Self-executiveness. Finally, the applicability of the Covenant might be put into question by the declaration made on the occasion of the ratification of the Covenant, namely 'that the provisions of articles 1 through 27 of the Covenant are not self-executing'. However, this declaration does not divest these provisions of their internationally binding effect; it merely serves to limit their domestic applicability and the generation of subjective legal positions in domestic law. The declaration cannot undermine the binding character of the Covenant rights under international law.[45]

Right to privacy: Article 17 ICCPR

The question is therefore, which legal framework does the Covenant set for surveillance measures? The provision of primary relevance[46] here is Article 17 ICCPR, according to which '[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or

[43] M Nowak, *UN Covenant on Civil and Political Rights*, (2nd edn, NP Engel Publishers, Kehl, Strasbourg and Arlington, TX, 2005) art 4, paras 12ff.

[44] CCPR, General Comment No 29, 31 August 2001, UN Doc CCPR/C/Rev.1/Add.11, paras 2ff.

[45] GA Sinha, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' (2013) 59 *Loyola Law Review* 861, 904.

[46] This is not exclusive. Further potentially affected human rights include the rights to freedom of expression, to liberty, to health, to work, to the highest attainable standard of living, and to equality and non-discrimination, see C Kent, L McGregor, D Murray and A Shaheed, 'Embedding Human Rights in Internet Governance' (3 November 2015) *EJIL Talk*, see <www.ejiltalk.org>, accessed 2 February 2016; insisting on the implications of the non-discrimination see also United Nations High Commissioner for Human Rights, Report on 'The Right to Privacy in the Digital Age', at (n 23) para 35ff.

correspondence'. Article 17(2) grants everyone the 'right to the protection of the law against such interference or attacks'.[47]

By using the general term 'correspondence', the Covenant does not distinguish between written, oral, electronic, visual, haptic or other forms of correspondence. As the Committee noted in its General Comment No 16, Article 17 ICCPR protects the integrity and confidentiality of all forms of communication: 'Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wiretapping and recording of conversations should be prohibited.'[48] Article 17 ICCPR prohibits 'arbitrary or illegal' interferences. Even interferences that are based on a domestic statute, such as FISA in the US, must not be arbitrary,[49] that is, they must be undertaken 'in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances'.[50]

Against this background, the Committee applied the Covenant and in particular Article 17 to the surveillance measures and urged the US to uphold its obligations to the implementation of the Covenant.[51] In detail, the Committee requested a redesign of the measures within the following parameters:

- Respect for the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance;
- Respect for the requirement of a legal basis;

[47] For the protection of privacy in the framework of the European Convention for the Protection of Human Rights and Fundamental Freedoms, see European Court of Human Rights, Grand Chamber, Judgment of December 4 2015, *Zakharov v Russia* (47143/06).

[48] CCPR, General Comment No 16, 8 April 1988, UN Doc HRI/GEN/1/Rev.9, para 8; see also the Report on surveillance of communication of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, La Rue, 17 April 2013, UN Doc A/HRC/23/40.

[49] On the cumulative character of the requirement, see Joseph and Castan (n 32) paras 16, 10ff.

[50] CCPR, GC No 16, see (n 48) para 4; therefore it is unclear which legal gap the initiative identifies that seeks to modify the ICCPR by way of amendment or addition.

[51] CCPR, Concluding Observations on the US, see (n 22) para 22: 'The State party should: (a) take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance; (b) ensure that any interference with the right to privacy, family, home or correspondence be authorized by laws that (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise specifying in detail the precise circumstances in which any such interference may be permitted; the procedures for authorizing; the categories of persons who may be placed under surveillance; limits on the duration of surveillance; procedures for the use and storage of the

- Introducing precise criteria limiting the measures in substance as well as in duration;
- Establishing a statutory authorization procedure as well as procedures for the use and storage of the data collected;
- Strengthening judicial involvement and introducing effective monitoring mechanisms;
- Refraining from imposing mandatory retention of data by third parties;
- Ensuring access to effective remedies.

Current US practice does not comply with these recommendations. The temporal and substantive limits to surveillance contained in FISA are too vague. Also, differential treatment on the basis of nationality or place of residence is not compatible with the Covenant. Finally, effective remedies against abuse are absent.[52]

III. Structural elements of the Internet constitution

In the end, in its Concluding Observations on the US, the Committee was brief in its comments on the US' surveillance practice.[53] While this is certainly more than nothing, the Committee's approach fell short of capturing the fundamental character of the problem as it continued to treat crucial questions of global communication rights exclusively within the traditional framework that is primarily interested in subjective rights against state interference. This approach misconceives that the struggle over the transnational constitution of the Internet cannot merely be posited as a struggle of individuals against nation states as the need for regulation doesn't only arise from individual legal subjects defending their spheres of liberty against the encroachments of domestic, supranational or even global political systems, as classic constitutionalism envisages it. Rather, it is transnational legal challenges that are at issue – challenges that arise from societal structural conflicts which, by their very nature, are beyond the

data collected; and (iv) provide for effective safeguards against abuse; (c) reform the current system of oversight over surveillance activities to ensure its effectiveness, including by providing for judicial involvement in authorization or monitoring of surveillance measures, and considering to establish strong and independent oversight mandates with a view to prevent abuses; (d) refrain from imposing mandatory retention of data by third parties; (e) ensure that affected persons have access to effective remedies in cases of abuse.'

[52] In addition, using embassies as surveillance posts is incompatible with the principle of sovereign equality of states under art 2(4) of the UN Charter and with the Vienna Convention on Diplomatic Relations and its Additional Protocol, art 3(1)(d) VCDR with art 1(1) AP (500 UNTS 95).

[53] These, by the way, are also not being respected by the German practice; on the legal issues, see Hoffmann-Riem (n 11).

individual.[54] The problem of protecting fundamental rights and democracy in the transnational constellation requires answers that transcend statist and legal-subjectivist reductionism.

Fundamental rights

The protection of the integrity of communication systems is a fundamental rights question that concerns the autonomy of communications processes. Unlike human rights protecting the physical and psychological integrity of individual corporeality, the protection of communicative spheres is directed at problems of societal communication that are structured quite differently, by (a) guaranteeing institutional autonomies and (b) developing personal spheres for enabling within the framework of these autonomies.[55]

Protection of systems: Institutional autonomies. First, this requires the radical de-individualisation of communication rights, especially with respect to guaranteeing the confidentiality and integrity of IT systems, which are particularly affected by the surveillance measures. It is therefore necessary to disconnect the protection objective of the liberties concerned from their relation to the individual.[56] Individual rights are no longer the starting point of the evolution of protection objectives; rather, they function as a procedural means of enforcement – legal subjects become advocates of un-individual rights, which provide subjective entitlements not in substantive terms but in a procedural sense. The individual right becomes the annex to an un-individual fundamental right.[57] As Wolfgang Hoffmann-Riem

[54] For the concept of transnational law see already PC Jessup, *Transnational Law* (Yale University Press, New Haven, CT, 1956) 2; for actual case studies and empirical evidence see e.g. the contributions in G Shaffer (ed), *Transnational Legal Ordering and State Change* (Cambridge University Press, New York, NY, 2013) and TC Halliday and G Shaffer (eds), *Transnational Legal Orders* (Cambridge University Press, New York, NY, 2015).

[55] On the differences between fundamental and human rights, see G Teubner, 'The Anonymous Matrix: Human Rights Violations by "Private" Transnational Actors' (2006) 69 *Modern Law Review*, 327.

[56] It cannot be emphasised enough that, of course, liberty also has to be secured in the relationship between the individual and Internet communication, especially with respect to a socio-digital subsistence minimum and individual guarantees, as e.g. proposed by H Maas, 'Unsere digitalen Grundrechte', *Die ZEIT*, 10 December 2015; but these individual rights have to be complemented by a structural attempt to secure social autonomies.

[57] O Lepsius, 'Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft' in F Roggan (ed), *Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008* (Berliner Wissenschaftsverlag, Berlin, 2008) 21–56 – dealing with the fundamental right, developed by the German Federal Constitutional Court, to a guarantee of the confidentiality and integrity of IT systems (BVerfGE 120, 274).

puts it: 'In the area of global communication structures, the protection of communication firstly depends on the protection of the system.'[58]

The Committee does not yet sufficiently take into account that the protection against surveillance measures is not primarily about keeping the individual private sphere free from state intervention. Rather, autonomous societal communication processes also have to be protected from the usurpation by other societal communications processes. This requires a more complex concept of fundamental rights, which no longer forces scopes of protection and situations of interference into the schema of private/societal vs public/statist. This framing does not live up to the transformations of the relation between private and public. The critical issue of transnational constitutionalism is not just binding domestic security organisations[59] or global security apparatuses[60] to fundamental rights. With respect to the Internet constitution, both of these variations of an 'international law of the Internet' reduce the constitutional question to the containment of political violence.[61] The new constitutional question is much more comprehensive. Whereas the old constitutional question concerned the justification and limitation of political violence,

> [w]ith the new constitutional question, the concern is to release quite different social energies – particularly visible in the economy, but also in science and technology, medicine and the new media – and to effectively limit their destructive effects.[62]

With respect to the surveillance of the Internet, the challenge is thus to both protect the communications systems from the encroachment of other societal functional spheres and, at the same time, to protect these functional spheres from being threatened in their integrity by a net communication that is oriented toward maximising its own rationality. Put differently, the Internet must be protected from the global functional systems such as politics, science, the economy, etc. But vice versa, the Internet constitution also has to protect these spheres from encroachments by Internet communication. The 'private sphere' of Internet communication

[58] W Hoffmann-Riem, 'Globaler Auftrag: Der Schutz der Freiheit vor staatlichen Eingriffen wie vor privaten Oligopolen muss in der digitalen Welt neu gefasst werden', *Frankfurter Allgemeine Zeitung*, 25 June 2014 (my translation).

[59] This is the approach of J Habermas, *The Divided West* (Polity Press, Cambridge, 2006) 115ff.

[60] This is the conception of B Fassbender, *The United Nations Charter as the Constitution of the International Community* (Brill Nijhoff, Leiden, 2009).

[61] See also P Kjaer, *Constitutionalism in the Global Realm: A Sociological Approach* (Routledge, London and New York, NY, 2014) 136ff.

[62] G Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford University Press, Oxford, 2012) 1.

thus acquires a public function and an obligation to the public. The public character of the sphere of Internet communication is its intrinsic normativity in relation to society, to human individuals, and to ecology. Private/public is therefore not a schema of differentiation between private subjects of law and public statehood, but in a polycontextural society refers to the fact that the (private) integrity of autonomous societal spheres has to be coupled with the (public) world society context in such a manner that one sphere enables the freedom of the other sphere.[63] Freedom is the freedom of the others, a constitution is a mechanism of dependency.[64] It constitutively binds together societal spheres of autonomy.

Horizontal effect of fundamental rights. In light of this, not only state and para-state sovereign acts require justification. Rather, the challenge is also to curtail polycentric societal spheres in their destructive tendencies so as to enable the curtailing of violence beyond the traditional regulatory formats of classic international law. The need for this reveals the gap in the Human Rights Committee's Concluding Observations, as the question of how the expansive tendencies of globally operating communication media can be effectively countered remains unanswered.

To conceive the constitutional curtailment at the transnational level according to the public character of the actor,[65] falls just as short as identifying International Public Authority with coercive forms of action.[66] The intensity and scope of the binding character of fundamental rights result neither from intrinsic characteristics of the actors nor from reasons innate to their action, but from societal structures, which the law reconstructs as public legal relationships – as the case may be, with corresponding duties and obligations. The point is to take seriously the fundamental rights dimension of the structural collisions of society and to concretise the legal requirements, starting from these collisions. This requires overcoming the question of who are the exclusive beneficiaries and obligated parties of fundamental rights. It calls for the development of structures that are able to adequately address the complexity described, structures that can counter the expansive tendencies of societal communication media appropriately,

[63] G Teubner, 'Societal Constitutionalism and the Politics of the Common' (2010) 21 *Finnish Yearbook of International Law* 111, 113–14.

[64] D Loick, 'Abhängigkeitserklärung. Recht und Subjektivität' in R Jaeggi and D Loick (eds), *Nach Marx: Philosophie, Kritik, Praxis* (Suhrkamp, Frankfurt, 2013) 296.

[65] A Peters, 'The Merits of Global Constitutionalism' (2009) 16 *Indiana Journal of Global Legal Studies* 397.

[66] A von Bogdandy, R Wolfrum, J von Bernstorff, P Dann and M Goldmann (eds), *The Exercise of Public Authority by International Institutions. Advancing International Institutional Law* (Springer, Heidelberg, 2010).

by way of organisation and reinforcement of self-limitating procedures.[67] This is true for the harmful effects on society of an unfettered global economy just as much as it concerns the dangerous maximisations of the rationality of the health system, of the law, of religion, of science and the media.

No sector is exempt from the responsibility of being responsive to the needs of global society. However, it would be a mistake to draw a simple analogy and apply the fundamental rights obligations designed for the Big Brothers, from the NSA to the Federal Intelligence Service, par for par to the Big Sisters, from Google to Facebook, without doctrinal adaptations. This would be too direct a transfer of fundamental rights, originally state-orientated, into other societal spheres. Instead, procedural solutions have to be developed that oblige both state and non-state actors to organise the protection of fundamental rights, each in their own way.

Some first steps toward such a new framework are gaining momentum in international legal practice, not least by the UN Human Rights Committee. In its General Comment No 16, it stated that the rights protected by Article 17 ICCPR have to be guaranteed against attacks and interferences irrespective of 'whether they emanate from State authorities or from natural or legal persons'.[68] Also, the former Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, has emphasised the obligations of the various sectors in society to respect data protection provisions,[69] basing himself on the respect, protect and remedy triad of obligations developed in the Ruggie Report.[70] This line of argument is explicitly carried forth by the actual Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye.[71]

[67] I Hensel and G Teubner, 'Horizontal Fundamental Rights as Collision Rules: How Transnational Pharma Groups Manipulate Scientific Publications' in K Blome, A Fischer-Lescano, H Franzki, N Markard and S Oeter (eds), *Contested Regime Collisions: Norm Fragmentation in World Society* (Cambridge University Press, Cambridge, 2016, forthcoming); this means also that new forms of accountability have to be developed; cf. the discussions about the accountability regime in the context of ICANN: IANA Stewardship Transition Coordination Group (ICG), *Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community*, October 2015.

[68] CCPR, GC No 16 (see n 48) para 1; on the horizontal effect, see also Nowak (n 43) art 2, at para 20; and Joseph and Castan (n 32) paras 1106ff.

[69] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 48) paras 72–77.

[70] J Ruggie, Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, 21 March 2011, UN Doc A /HRC/17/31.

[71] D Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 22 May 2015, A/HRC/29/32, para 62ff.

In respect to global surveillance measures, unfortunately, the UN Human Rights Committee is less interested in this non-state dimension of surveillance – not a word has been written on the liability exemptions contained in FISA for the involvement of private actors in surveillance measures, which constitute a violation of the obligation to protect fundamental rights;[72] nor a word on the extraterritorial obligations to surrender information, which are being enforced also against US companies in Europe, despite well-meaning Safe Harbor agreements;[73] and finally, no mention has been made of the corporate due diligence obligations developed in the Ruggie Report, following a network of transnational codes, from the UN Global Compact's ten universal principles and the G3 Guidelines of the Global Reporting Initiative, to the ISO 260000 on Social Responsibility of the International Organization for Standardization, the ILO Declaration on Fundamental Principles and Rights at Work and the OECD Guidelines for Multinational Corporations.

All of these initiatives promote respect for human rights among private actors,[74] and – as the Guiding Principles state – they clarify the 'role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights'.[75] International and transnational arbitral tribunals, too, have long begun, in the area of *lex digitalis publica*, to bind private actors to specific fundamental human rights.[76] And even the CJEU, in its pragmatic

[72] See CJEU (n 9), *Maximillian Schrems v Data Protection Commissioner*, para 94: 'In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter'.

[73] US District Court for the Southern District of New York, 25 April 2014 – Memorandum and Order In The Matter Of A Warrant To Search A Certain E-Mail Account Controlled And Maintained By Microsoft Corporation (USDC, 13 Mag 2814).

[74] Details in SD Murphy, 'Taking Multinational Corporate Codes of Conduct to the Next Level' (2005) 43 *Columbia Journal of Transnational Law* 389; see the CCPR's Resolution of 26 June 2014, UN Doc A/HRC/26/L.22, on the 'Elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights'.

[75] Ruggie, Guiding Principles (n 70), preamble; see also European Parliament, Committee on Foreign Affairs, M Schaake, Report on 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights and Third Countries', 3 June 2015, A8-0178/2015, para 32: 'Reminds corporate actors of their responsibility to respect human rights throughout their global operations, regardless of where their users are located and independently of whether the host state meets its own human rights obligations; calls on ICT companies, notably those based in the EU, to implement the UN Guiding Principles on Business and Human Rights, including through the establishment of due diligence policies and risk management safeguards, and the provision of effective remedies when their activities have caused or contributed to an adverse human rights impact'.

[76] See L Viellechner, *Transnationalisierung des Rechts* (Velbrück, Weilerswist, 2013) 259ff.

manner of binding non-state actors to fundamental rights via the general principles of EU law, has asserted that Google is bound by the European Charter of Fundamental Rights:

> Inasmuch as the activity of a search engine is therefore liable to affect significantly … the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements … in order that the guarantees … may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.[77]

The cooperation between governments and private actors worldwide in the digital domain evokes the need to reconsider the very concept of human rights as individual rights. Self-evidently, '[i]nternet governance should be framed around fundamental human rights principles, in particular transparency, openness, inclusivity, non-discrimination and equality, and should incorporate the right to an effective remedy'.[78] But the fact that Internet communication and big data enhance 'the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern',[79] is not only problematic as it affects individual rights,[80] but above all as the transnational constellation poses new challenges to our understanding of fundamental rights.

As the UN Human Rights Committee is only interested in these crucial questions of global fundamental rights protection within the traditional framework, which seeks to defend subjective liberties against state encroachment, it cannot give direction for the regulation of complex societal

[77] CJEU, *Google Spain* (n 21) para 38; see also ibid, para 81: 'In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing.'

[78] C Kent, L McGregor, D Murray and A Shaheed, 'Embedding Human Rights in Internet Governance' (n 46).

[79] UN Human Rights Council, The Right to Privacy in the Digital Age, A1 April 2015, A/HRC/RES/28/16, at 2.

[80] See the mandate of the Special Rapporteur on the Right to Privacy as expressed in Human Rights Council, ibid, at 3ff, and the mandate explication by J Cannataci who was appointed special rapporteur in July 2015, see OHCR, Special Rapporteur on the right to privacy, available at <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>, accessed 2 February 2016.

structural conflicts such as those manifested in the global surveillance measures. This inappropriate framing falls short of adequately translating the societal structural conflict into law. It also obstructs the view to possible solutions for this conflict.

Democracy and public control

As a consequence, the Committee also ignores the transnational dimensions of the democratic question raised by the case of the global surveillance measures.

It is often enunciated that 'cooperation between governments and private actors worldwide in the digital domain, including the Internet Governance Forum, calls for clear checks and balances and must not lead to the undermining of democratic and judicial oversight'.[81] But what remains unresolved is the question of the adequate structures for this oversight to be performed efficiently.

If Internet governance is – as in the Tunis Declaration[82] – defined as 'the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet',[83] then it is obvious that the democratic question goes beyond the question of states' democracy. In the transnational constellation it affects all spheres of Internet governance: civil society, multistakeholder processes like NETmundial, International Organisations and hybrid forms of collaboration.

The crucial point here is that for those flexible networks and organisations, adequate procedures and forms for self-limitation must be developed, by which societal communication spheres are organised democratically. In its Concluding Observations, the UN Human Rights Committee focuses on the requirement of a domestic legal basis. This is an important building block in a system of self-regulation of functional spheres, but it stops short of the self-limitation of politics. In the transnational constellation, however, democratic requirements must also be enforced in relation to other actors

[81] European Parliament, Committee on Foreign Affairs, M Schaake, Report on 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights and Third Countries' (n 75) para 58.

[82] The Tunis Summit in 2005 was one of the outcomes of Resolution 56/183 (2001) of the UN General Assembly, which welcomed the creation of an intergovernmental World Summit on the Information Society ('WSIS').

[83] Tunis Agenda for the Information Society, 18 November 2005, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, para 34; see also United Nations General Assembly's Overall Review of the Implementaion of WSIS Outcomes, Zero Draft, October 2015, para 32.

aside from states. In the area of global communication structures, the monopoly of information

> becomes a problem for the constitution of the new media which cannot be reduced to economic issues. Its worldwide digital networking activities, which have enabled massive intrusions into the rights to privacy, informational self-determination and freedom of communication, represent typical problems for the constitution of the global Internet. And the lack of transparency in Google's governance structures points to constitutional questions of democracy and of public controls.[84]

These constitutional questions cannot simply be answered by tightening the net of partial democratic legitimation through the nation states.[85] Rather, the principles of democracy and of public control need to be anchored and, if necessary, legally enforced within the polycentric patterns of order themselves.[86] For example, this applies to the data protection standards of Google,[87] but also to the practice of Wikileaks,[88] which has recognised rights set out in the Universal Declaration of Human Rights in their 'harm minimization procedure'. Such procedures provide for the deletion of information in the case that 'life and limb of innocent people' require protection.[89]

It is in this ultra-cyclical link between private standards and international legal codifications that we find untapped potential for the development of societal constitutionalisation processes. This, however, requires the institutionalisation of reflexive processes and procedures that allow via secondary norms for the enactment, modification, interpretation and

[84] G Teubner, 'The Project of Constitutional Sociology: Irritating Nation State Constitutionalism' (2013) 4 *Transnational Legal Theory* 44, 44–5.

[85] Cf European Parliament, Committee on Foreign Affairs, M Schaake, Report on 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights and Third Countries' (n 75) para 58; but see J Bast, 'Das Demokratiedefizit fragmentierter Internationalisierung' in H Brunkhorst (ed), *Demokratie in der Weltgesellschaft*, special issue no 18 of *Soziale Welt* (Nomos, Baden-Baden, 2009) 185–93.

[86] C Thornhill, 'A Sociology of Constituent Power: The Political Code of Transnational Societal Constitutions' (2013) 20 *Indiana Journal of Global Legal Studies* 551.

[87] See Google, Privacy Policy, last updated 30 June 2015, available at <http://www.google.com/policies/privacy/>, accessed 2 February 2016.

[88] Wikileaks, Standard Operating Procedures, para 1, available at <https://wikileaks.org/About.html>, accessed 2 February 2016: 'We derive these principles from the Universal Declaration of Human Rights. In particular, Article 19 inspires the work of our journalists and other volunteers. It states that everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. We agree, and we seek to uphold this and the other Articles of the Declaration.'

[89] Ibid, para 1.2.

implementation of the primary norms. Monitoring and implementation bodies need to be established, tasked with mediating between the abstract corporate principles and the concrete corporate decisions.[90]

Such procedures do not spring forth spontaneously and fully formed. Indeed, it requires external and internal pressure and, if need be, judicial advocacy and control to be exerted if Codes of Conduct are to be more than PR strategies, for a Safe Harbor initiative such as the EU's[91] not to end up as a mere merchandising instrument.[92] A strengthening of self-limiting procedures can be achieved by introducing institutionalised forms of self-regulation, through political control. Such externally regulated self-regulation is distinct from deregulation in that it doesn't renounce control in a *laissez-faire* manner, but introduces binding, even judicial control mechanisms that combine internal and external monitoring bodies.[93]

The first steps in this direction have been made, for instance, by strengthening transparency through reporting duties for businesses with respect to human rights scenarios, or by requiring the establishment of Corporate Social Responsibility institutions.[94] Only when these mechanisms and institutions are obliged to cooperate with politically established institutions – penal and administrative agencies, domestic courts, national and international human rights bodies – can a network of legal control develop in which legal norms become effective. This requires the adjustment of an asymmetrical judicialisation, as a result of which private actors and transnational corporations can enforce their claims in various international forums, most notably courts of arbitration, while it is virtually inconceivable that they will ever find themselves in the position of defendant in the forums of global justice.[95] Their partial recognition as subjects of international law results in an entitlement under international law without sufficiently effective corresponding obligations. Only if these gaps are closed by a

[90] G Teubner, 'Self-constitutionalizing TNCs? On the Linkage of "Private" and "Public" Corporate Codes of Conduct' (2011) 18(2) Indiana Journal of Global Legal Studies 617.

[91] On the inefffectiveness of this mechanism and the concluding violation of fundamental rights see CJEU (n 9), *Maximillian Schrems v Data Protection Commissioner*, para 94ff; for a critical assessment, see also P Schaar, 'Lässt sich die globale Internetüberwachung noch bändigen?' (2013) 46 *Zeitschrift für Rechtspolitik* 214–16.

[92] See the criticism in J Seeger, 'To cloud or not to cloud. Editorial' *iX. Magazin für professionelle Informationstechnik* 11/2011: 'that these provisions aren't worth the paper they are printed on' (my translation).

[93] To this effect G Teubner, 'Substantive and Reflexive Elements in Modern Law' (1983) 17 *Law and Society Review* 239.

[94] S Deva, *Regulating Corporate Human Rights Violations: Humanising Business* (Routledge, London and New York, NY, 2012) 96.

[95] J von Bernstorff, 'Die UN Guiding Principles on Business and Human Rights', November 2012, available at <https://www.unesco.de/wissenschaft/2012/uho-1112-keynote-bernstorff.html>, accessed 2 February 2016.

combination of internal and external control mechanisms can a juridification develop that is powerful enough to enforce the promises of the Codes of Conduct and of the Corporate Social Responsibility initiatives.

Beyond establishing opportunities for control and participation that link the levels of the organisation with societal constitutions, the preconditions for forming a democratic public must be secured.

Empowering a critical public. This requires first and foremost that a critical public can find spaces to bring such concerns to attention.[96] However, the UN Human Rights Committee has shown little interest in the question of transnational control mechanisms, as the suppression of whistleblowing and restrictions on democratic procedures are not discussed in its Concluding Observations. Even though the shadow reports to the US state report called for substantive protection for whistleblowers with reference to Article 19 ICCPR,[97] the Committee chooses to ignore the matter entirely.

Whistleblowing is a crucial mechanism that promotes democratic control.[98] By ignoring this dimension, the UN Human Rights Committee misses an important opportunity to develop a legal framework through which democratic forces may impel greater regulation of the actions of the state. If, as Foucault developed in his critique of Bentham,[99] the total control of the network of the security apparatuses isn't to be replaced by a panoptic scheme from below, there must of course also be limits to whistleblowing.

[96] GW Anderson, 'Societal Constitutionalism, Social Movements, and Constitutionalism from Below' (2013) 20 *Indiana Journal of Global Legal Studies* 881.

[97] E.g., see the Shadow Report by the NGO 'Article 19' for the October 2013 session of the UN Human Rights Committee: 'Protecting whistleblowers that hold governments and institutions to account is central to protecting the right to freedom of expression under international law, available at <https://www.article19.org/resources.php/resource/37185/en>, accessed 2 February 2016.

[98] G Teubner, 'Whistle-blowing in the Stampede? Comment on B Frey and R Cuenis, 'Moral Hazard and Herd Behaviour in Financial Markets' in S Grundmann, F Möslein and K Riesenhuber (eds), *Contract Governance* (Oxford University Press, Oxford, 2015) 100–5; see also Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs, Report: 'Mass Surveillance', Rapporteur Pieter Omtzigt (n 39) para 122: 'But even after appropriate legal limits and oversight mechanisms have been established on the national level and on the international plane in the form of a multilateral "intelligence codex", whistle-blowing will be needed as the most effective tool for enforcing the limits placed on surveillance. The activities of secret services are by nature difficult to scrutinise by any of the usual judicial or parliamentary control mechanisms. Access of any monitoring bodies to relevant information and capacity issues in view of the huge volume of activity to be monitored will always remain a problem for effective supervision. The "sword of Damocles" of the disclosure of any abuses by well-protected inside whistle-blowers may well constitute the most powerful deterrent against serious violations of the legal limits that should in our view be placed under surveillance.'

[99] Foucault (n 7) 195ff.

However, these limits cannot be determined by the needs of politics or the military; rather, they must themselves be at the disposition of the democratic process.[100]

A Right to encryption. But the democratic question does not only call for a societal wide discussion of surveillance. A process of double reflexivity must be organised, in order to enable emancipation from the panoptic schema. The function of the constitution results from the very fact that it links reflexive processes of the law to reflexive processes of society. Politics is limited and constituted by a political constitution, the economy by the economic constitution, and so on. It is the very point of the constitutional idea that any constitution, while legally regulating the formation of law, also releases self-limiting forces.

Edward Snowden alludes to how this can be achieved for the Internet constitution when he replaces the idea of limiting power by the constitution with the idea of limiting power by cryptography, following Thomas Jefferson's response to the question of political power:

> While I pray that public awareness and debate will lead to reform, bear in mind that the policies of men change in time, and even the Constitution is subverted when the appetites of power demand it. In words from history: Let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography.[101]

Contrary to Snowden's view, though, a constitution and cryptography are not mutually exclusive. To the contrary, cryptography must form a central element of the Internet constitution. In the reflexive application of the digital code to itself and in its linkage to a constitutionally protected right to use encryption, a capillary constitution of Internet communication develops. Cryptography becomes an element of a 'constitutionalization from below', in which the users overcome the panoptic schema. The fundamental right to cryptography and the free choice of encryption methods emanate from the right to privacy. This right must therefore also grant protection against prosecution based on the use of cryptography. The right to resist surveillance necessitates a counterbalance of a constitutional right to digital self-defence. This results in a duty – applicable to states and corporations – to promote opportunities for using cryptography.

[100] A Fischer-Lescano, 'Putting Proportionality into Proportion: Whistleblowing in Transnational Law' in K Blome *et al.* (n 67).

[101] E Snowden, cited after C Friedersdorf, 'Edward Snowden's Other Motive for Leaking', *The Atlantic*, 13 May 2014. The well-known original quote goes: 'In questions of power, then, let no more be heard of confidence in man, but bind him down from mischief by the chains of the Constitution.'

Consequently, in their 'Resolution in Support of the Freedom to Use Cryptography', the members of the Global Internet Liberty Campaign (GILC) emphasise that the right to an unhindered use of cryptographic technologies flows from the right to privacy.[102] That legal access to encryption technologies and effective protection of the use of such technologies are crucial issues in the enforcement of the right to privacy, is also highlighted in the OECD Cryptography Policy Guidelines,[103] as well as in the Common Statement on Cryptography by the International Working Group on Data Protection in Telecommunication (IWGDPT).[104] While the UN Human Rights Committee has yet to take a position on this, the challenge will be to extend the scope of protection of Article 17 ICCPR to such forms of constitutionalisation of the Internet.[105]

Cryptography modifies the panoptic schema and allows for the anonymisation of data and communication. It is part of a strategy to establish breaks, vision barriers and protection measures through the *chains of social constitutions* that foster the self-limiting procedures of social systems. In the end, the liberty safeguards that Foucault envisages in his critique of the panoptic schema[106] can only be established by way of a

[102] Global Internet Liberty Campaign (GILC), Resolution in Support of the Freedom to Use Cryptography, September 25, 1996 (Appendix B); on the right to cryptography as a 'right to be unheard' under US law, see PE Reiman, 'Cryptography and the First Amendment: The Right to be Unheard' (1996) 14 *John Marshall Journal of Computer & Information Law* 325; for a German perspective, see J Gerhards, *(Grund-)Recht auf Verschlüsselung?* (Nomos, Baden-Baden, 2010).

[103] OECD Cryptography Policy Guidelines. Recommendation of the Council Concerning Guidelines for Cryptography Policy, 27 March 1997.

[104] International Working Group on Data Protection in Telecommunication (IWGDPT), Common Statement on Cryptography, 12 September 1997.

[105] See also D Kaye, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 71), who insists on the implication of art 17 ICCPR (para 16ff) and concludes (para 62ff): 'At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers. The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption by design and default to users around the world'.

[106] Foucault (n 7) 195ff.

combination of constitutional limitation and visibility refraction; only in this way can the architecture of the transnational panopticon itself be changed, and only in this way is the core of the issue addressed: that the subtle mechanisms of societal energies (here, of Internet communication) have to be at once released and limited in their destructive effects.

IV. Conclusion

In its Concluding Observations to the 2014 US state report, the UN Human Rights Committee recalled essential preconditions for the regulation of global communication structures. It correctly emphasised the extraterritorial effect of fundamental rights and urgently called for proportionality in the use of extraterritorial surveillance measures, in accordance with law.

However, thus far the Committee has yet to thoroughly engage with issues resulting from transnational surveillance practice beyond subjective rights vis-à-vis state encroachment. However, as it has now become clear, the legal issues of the Internet constitution are too complex to be dealt with in this regulatory framework alone. The search for contemporary forms of protection for the integrity of communicative systems and the defence against threats from anonymous societal matrices requires in-depth engagement with world-society structural conflicts. The constitutional challenge is therefore, to enable the release and limitation of societal energies in a way that is adequate to their subject matter, beyond the state system of society. Consequentially, a framework for the horizontal effect of fundamental rights must be developed that takes into account democratic questions of procedures and forums in which societal self-normation practices can be institutionalised.

The Internet and email communication have only existed for about 30 years. In order to ensure that legal frameworks remain responsive to modern realities, the centuries-old *ius inter gentes* of the Westphalian state system must be advanced. If international law is to make a contribution to the struggle over the Internet constitution, our understanding of international public law needs to evolve alongside transnational forms of power generated by societal communication media beyond how we understand international law today – beyond the traditional political sphere. These regulation efforts must overcome subjectivist and statist reductionism, in order to be able to take such problematic constellations into account if we are to defend and protect human rights against an ever-encroaching global panopticon.