

Re-Constituting Global Cyber-Law

*Thomas Streinz**

Note for IILJ Colloquium 2018: “International Law of Google”

This paper has been through various iterations. For the IILJ Colloquium 2018 “International Law of Google” I wrote an almost entirely new and short version to reflect my current thinking and to test (and subsequently revise and refine) some rather bold claims. I welcome your feed-back and pushback and look forward to our discussion.

Abstract

This short paper seeks to re-constitute global cyber-law as a globally applicable body of rules, norms, and practices to effectively steer stakeholders with significant decision-making power in Internet governance. This builds on insights from Global Administrative Law (GAL) but adapts them to the unique context of global Internet governance to advance ‘global law’ theory and practice.

* Fellow, Institute for International Law and Justice, NYU Law. Email: thomas.strein@law.nyu.edu.

Earlier (and rather different) versions of this paper were presented at the Association of Internet Researchers (AoIR) Annual Conference in Berlin in October 2016, at the Hauser/Emile Noël Global Fellows Forum at NYU Law in March 2017, and at the Fifth Annual Conference on Governance of Emerging Technology at ASU in Phoenix, Arizona in May 2017. I am indebted to Gráinne de Búrca, Daniel Francis, Benedict Kingsbury, Paul Mertenskötter, Ingolf Pernice, Johann Justus Vassel, and Joseph Weiler for invaluable critique, comments, and suggestions.

I. Introduction

Vint Cerf, the famous three-piece-suit wearing founding father of the Internet, sounded the alarm in the Financial Times in February 2018: ‘Rebuild internet governance before it is too late’.¹ He lamented that “[m]anaging the way that a large number of separate legal frameworks apply to the internet is one of the big policy challenges of our time and is more complex even than building the internet.” He endorsed the efforts of the Internet and Jurisdiction Policy Network, a multi-stakeholder organization comprised of governments, international organizations, technical operators, civil society, and academia to find solutions to a fundamental yet unresolved question of Internet governance: how to square the right of states to create and enforce laws within their jurisdictions (and beyond) with the idea of transnationally interconnected networks that are together ‘the Internet’?²

This short paper argues that re-constituting a ‘global cyber-law’, i.e. a body of principles, rules, and practices applying to those who wield power in Internet governance, is essential to achieve the normative goal of an open and global Internet. This ‘global cyber-law’ is meant to hold both code- and law-makers accountable irrespective of long established but outdated distinctions between public and private entities. It incorporates and interacts with domestic and (traditional) international law without claiming a hierarchical superiority. Its force is gravitational rather than coercive. Yet, it fulfills crucial rule of law functions essential for legitimate and effective Internet governance.

By Internet governance, I mean any measure by states, international organizations, corporations, or technical standard-setting bodies affecting the evolution, operation, and use of the Internet, regardless whether such measures concern the physical layer of the Internet, i.e. the land- and sea-cables, antennas, satellites, routers, and servers through which the information flows, its logical layer, i.e. the

¹ Vint Cerf, Rebuild internet governance before it is too late (Financial Times, February 20, 2018), <https://www.ft.com/content/e1e6d1e0-156c-11e8-9c33-02f893d608c2>.

² This paper retains the capitalization of ‘the Internet’, treating it as a proper noun, to emphasize that ‘the Internet’ is not just any interconnected network but *the* TCP/IP based solution to the problem of inter-networking that emerged as the dominant standard world-wide. See further *infra* II.A.

protocols that organize the information flow, or its content layer, i.e. the actual information that is being transmitted.³ This maintains a distinction between measures that affect the Internet's functioning at the physical and logical layers (such as the operation of the Domain Name System, DNS, or changes to the Internet Protocol, IP) on the one hand, and measures that affect user conduct on the other hand, for analytical and conceptual reasons even though both are part of Internet governance and intricately intertwined.

My larger project, of which this short paper forms a part, speaks to and engages with different audiences in an attempt to bring together, cross-fertilize, and criticize the discourse among scholars and practitioners of Internet governance, 'cyberlaw', international law, and 'global law'. It calls on the various stakeholders in Internet governance venues such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) to re-evaluate their outdated perception of 'law' as a necessarily state-made creature and to embrace it as an important tool to lend legitimacy and accountability to institutions that fulfill key functions in Internet governance. It seeks to revitalize the 'cyberlaw' debate by breaking it out of often insular jurisdiction-specific discourses, by taking Larry Lessig's 'code is law' insight seriously, and by bridging the divide between 'exceptionalists', who believe that the Internet *is* different and requires novel approaches to governance and regulation, and 'unexceptionalists', who believe that established jurisdictional principles are able to govern transnational information exchange via the Internet.⁴ It urges international lawyers to move beyond the ongoing (but ultimately rather pointless) debates about the application of (traditional) international law in or to 'cyber-space', to critically re-evaluate ongoing efforts to constrain the policy space for Internet governance via comprehensive economic agreements such as the Trans-Pacific Partnership (TPP), and to explore the extent to which treaties and custom can become building blocks of 'global cyber-law'. Most importantly, it encourages proponents, theorists, and

³ This is modelled after the definition of Internet Governance that came out of the World Summit on Information Society (WSIS) 2005: "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 programs that shape the evolution and use of the internet."

⁴ This distinction between exceptionalists and unexceptionalists is taken from David G. Post, *In Search of Jefferson's Moose. Notes on the State of Cyberspace* (OUP 2008), pp. 166-7.

practitioners of ‘global law’ to take the Internet seriously as an object of study and practice. Indeed, many of the phenomena that are increasingly conceptualized as ‘global law’ are made possible or are at least facilitated by the Internet, yet scholars of global law and governance have tended to study the consequences rather than the roots of these developments from a ‘global law’ perspective.⁵ In this sense, by developing a conception of ‘global cyber-law’ with a clear normative agenda and real-world implications, my project also tries to contribute to ‘global law’ theory and practice.

In this short paper, I am trying to re-constitute ‘global cyber-law’ by answering three basic questions: Is there a need for it? What is its content? And is it ‘law’? By trying to answer each of these questions, I tackle some predictable objections against the conception of global cyber-law that I advance in this paper. They are familiar from critics of different versions of ‘global law’ cannot be easily dismissed. But while these objections are useful as a corrective they ultimately fail to provide an alternative that is descriptively or normatively appealing.

The idea behind global cyber-law is to use ‘law’ to solve three basic problems of global Internet governance: The first is to hold decision-makers accountable that have significant power over the world’s most important information exchange technology. The second is how to coordinate the law-making and enforcement activities of nation states to the extent to which they have extra-jurisdictional implications for the Internet as a whole. The third is that the two problems are in fact interrelated as there is no neat separation of roles and responsibilities in Internet governance; the question then is how to coordinate the decision-making by the plethora of actors in the Internet governance universe?

My answer to these three questions is ‘global cyber-law’. Global cyber-law is *global* in the sense that its scope of application is detached from jurisdictional boundaries of nation states. To preserve and eventually realize the Internet’s global potential, the scope of cyber-law needs to be aligned with its object. Global

⁵ A notable exception is Eyal Benvenisti, EJIL Foreword: Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?, EJIL 2018 (forthcoming).

cyber-law is *cyber* in the literal sense of the world. It is designed to be ‘skilled at steering’ the Internet’s key stakeholders in their decision-making. Finally, global cyber-law is ‘law’ in demanding compliance because of its nature as ‘law’ and hence crucially relies on its recognition as such.

I am not claiming that global cyber-law already exists. I am arguing that it is needed and try to show what it might look like, why it matters that it is law, and how it might come about. I also claim that some glimmers of global cyber-law have always existed and that more building blocks are increasingly visible but that they need to be recognized as such to re-constitute global cyber-law.

II. The Need for Global Cyber-Law

Is there a need for ‘global cyber-law’? I will try to answer this question in two steps. The first is to identify the problems that global cyber-law is trying to solve. The second is to show why (only?) global cyber-law is able to solve them.

There are (at least) three problems in Internet governance in need of a solution. The first is the fact that several key decision-makers hold considerable power and influence over the world’s most important information exchange system without being subject to appropriate forms of accountability and control. The second is the challenge to retain (and if possible realize) the Internet’s global potential by coordinating the domestic and international law-making efforts of states to the extent to which they affect the Internet not just within their jurisdictions but beyond. The third problem is that these two problems are in fact interrelated even though the conventional definition of Internet governance conveys the unhelpful fiction that governments, the private sector, and civil society had neatly separated roles.⁶ In reality, Internet governance is a complex system in which stakeholders may participate in different venues in different ways, exerting varying degrees of influence and control. Resolving an issue in one venue might only exacerbate the

⁶ Supra note 3: “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 programs that shape the evolution and use of the internet” (emphasis added).

pressure to find a different, potentially contradictory solution in another. Let me illustrate this with a couple of examples:

- ICANN, the Internet Corporation for Assigned Names and Numbers, is in charge of the operation of the Internet's unique identifier system by administering the domain name system (DNS) and by coordinating the allocation and assignment of IP numbers.⁷ ICANN's domain name policies directly affect the domain name market where the registration of new domain names easily conflicts with established intellectual property rights (especially trademarks) but ICANN's policies may also be in tension with states' laws and policies regarding geographical indications, cultural heritage, or public morals. Control over the DNS—'ruling the root'—puts ICANN into a position of power over the Internet's key infrastructure. Theoretically, manipulation of the DNS could be used for content moderation by taking down domains that are used to transmit unwanted information. Its self-imposed restriction to refrain from such measures—even if 'human rights' are at issue—places the responsibility over Internet content into the hands of other stakeholders (mainly states and Internet platform corporations). Conversely, control over the DNS by ICANN limits the ability of states to monitor and modify the DNS to stave off cyberattacks (for which the DNS is—unwittingly—a key infrastructure). ICANN prides itself of its 'bottom-up consensus-based multistakeholder process' in which business interests, technical experts, governments, and civil society are involved. But the power of stakeholders to influence ICANN's decision-making varies widely. Even if there is an ICANN policy, governments retain the right to enact and enforce their laws within their jurisdictions—and business interests and civil society will seek to influence these efforts irrespective of ICANN's internal decision making.
- The Internet Engineering Task Force (IETF), an open standards organization operating under the auspices of the Internet Society (ISOC),

⁷ ICANN Bylaws, Article 1.1.

an international membership-based non-profit organization, controls the development of the Internet protocols. Its decision-making follows (theoretically) open processes leading to the adoption of standards via the famed ‘rough consensus and running code’ principle. Participants are ‘volunteers’, i.e. experts who are paid by their employers—often universities or large Internet corporations—to participate in IETF activities.⁸ These individuals exercise power over the Internet’s fundamental code, so to speak the ‘basic laws’ of the Internet, since compliance with these protocols is a condition sine qua non for information exchange via the Internet. Even though the IETF frames Internet protocol development as a purely technical exercise, its decisions have wide ramifications. When voice-over-IP telephony began to replace traditional over-the-wire phone calls, governments lost the ability to wiretap. The IETF considered but ultimately rejected the possibility to build ‘backdoors’ into the Internet protocols to facilitate governmental surveillance.⁹ Hence, governments had to find other ways to collect information, including via mandated (meta-)data collection by internet service providers (ISPs) and via requesting data directly from internet platform corporations. The fact that the IETF is effectively outside governmental control is widely celebrated within the Internet community. But this does not alleviate concerns about the IETF’s legitimacy and accountability in making decisions which affect billions of people around the globe. Conversely, where the IETF refrains from taking action (as in the wiretapping/backdoor discussion), governments will find other ways, thereby exacerbating the risk of divergent rules and regulations with the potential to undermine the Internet’s global potential.

- Quite naturally, states have different approaches to Internet policy and regulation, depending on their political systems, public values, stage of economic development etc. Nevertheless, historically, the EU and the US evolved as Internet law-makers with global appeal. The rapid expansion of

⁸ Nahuel Maisley, *Protocols as Global Law: A Critical Approach to the IETF’s Role in Regulating Our (Cyber-) Lives* (paper on file with author).

⁹ IETF Policy on Wiretapping, RFC 2804.

information flows via the Internet is often credited to liability exemptions in US law for communication platforms (intermediaries) that were widely copied in jurisdictions around the world.¹⁰ The EU successfully exported its privacy policies, first enacted via the 1995 Data Protection Directive and now being replaced by the General Data Protection Regulation, by exploiting the ‘Brussels effect’, i.e. gravitation to the highest standard for economic reasons, and by actively pushing other states to have ‘adequate’, i.e. functionally equivalent data protection laws.¹¹ Systematically, if one endorses the idea of a global Internet, global law-making by certain states is desirable (concerns over its legitimacy notwithstanding). The problem is that the EU and the US exercised this function without fully realizing what they were effectively doing and without appropriate involvement of Internet governance stakeholders outside their jurisdictions. In future, it seems likely that the rising digital powers (most notably China, but also Brazil and India) will increasingly chart their own course. The extent to which they will craft their own national Internet law and policy will in part depend on the ability of existing and possibly still-to-be-created global Internet governance institutions to include, accommodate, and mediate their interests.

- So called free trade agreements (FTAs) increasingly address questions of Internet law and policy such as access restrictions, free data flows, data privacy, server location requirements, source code protection, domain-name dispute settlement, and the liability of intermediaries. States enter into these agreements to increase legal certainty for the digital economy and incur external obligations that effectively constrain their ability to regulate at will. Crucially, most Internet governance stakeholders are shut out of the negotiations of FTAs, which are traditionally clouded in secrecy, while business interests, often organized in trade associations, are able to lobby trade ministries effectively. While ICANN’s transparent if cumbersome multi-stakeholder process has been laboring over a reform of

¹⁰ Section 230 of the Communications Decency Act; Section 512 of the Digital Millennium Copyright Act.

¹¹ Anu Bradford, *The Brussels Effect*, 107 *Northwestern University Law Review* (2012).

its Who-Is policies for years, the Trans-Pacific Partnership (TPP), also in its reincarnation as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), requires its participating states to provide ‘online public access to a reliable and accurate database of contact information concerning domain name registrants’ for country-code top-level domains (ccTLDs).¹²

- Giant Internet platform corporations such as Google, Amazon, Facebook, and Apple create vastly popular venues for economic and social exchange and as a consequence control most of the data in the global digital economy. The resulting position of power is increasingly in tension with the mantra that these are purely private for-profit corporations, mainly accountable to their shareholders. Even without formally regulating these platforms as public utilities, it seems clear that they provide functions in the public domain which have a tremendous impact on people’s life. Platform corporations engage in self-regulation (platform governance) to stave off regulatory intervention by states as their interest in providing a transnationally uniform product aligns with the idea of a global Internet. But states increasingly require platforms, by law, to engage in content moderation. Germany requires social networks with more than two million users to operate an effective and transparent process to resolve complaints about illegal content; ‘obviously illegal’ content must be removed within 24 hours.¹³ Following a decision by the EU Court of Justice, Google had to implement similar procedures to handle delisting requests (based on the misleadingly labelled ‘right to be forgotten’).¹⁴ The question whether de-listings need to be implemented globally or only within the territory of the EU is pending before the Court.¹⁵ On the other side of the Atlantic, the US Supreme Court is deliberating whether a domestic warrant is sufficient to access data stored abroad.¹⁶ Contrary to the unexceptionalist view, these

¹² TPP, Article 18.28.1(b).

¹³ *Netzwerkdurchsetzungsgesetz (NetzDG)*.

¹⁴ Case C-131/12, *Google Spain v AEPD and Mario Costeja González*, ECLI:EU:C:2014:317.

¹⁵ Case C-507/17, *Google Inc. v Commission nationale de l’informatique et des libertés (CNIL)*.

¹⁶ *United States v. Microsoft Corporation*.

instances are not just cases of conflicting jurisdictions. Internet platforms are key regulators themselves and need to be held accountable as such.

To reiterate, the reality of Internet governance creates power structures, in which certain key institutions are in need of accountability and control, in which states and international organizations enact and enforce their laws as if it would not affect other Internet stakeholders, and in which there is no way to effectively address and mitigate the resulting tensions within the system while preserving a globally interconnected Internet.

In my view, ‘global cyber-law’, understood as a global body of law that governs those who wield significant power in Internet governance, is at least one (if not the only) plausible solution to these problems. ‘Global cyber-law’ has the potential to hold key decision-makers in Internet governance more effectively accountable by requiring them to comply with basic procedural requirements of transparency, participation, reason-giving and review, which might not only improve their legitimacy but potentially also the outcome of their decision-making. Furthermore, ‘global cyber-law’ can help to address the problem of conflicting extra-jurisdictional law enactment and enforcement by states and international organizations by requiring them to consult with other Internet governance stakeholders and to take the effects of unilateral extra-jurisdictional law-making into account. In sum, ‘global cyber-law’ provides a holistic framework and common language for Internet governance decision-makers across different venues.

At its core, this is a ‘rule of law’ argument.¹⁷ Even though there is no globally uniform understanding, let alone definition, of the ‘rule of law’, the idea that arbitrary exercise of power is normatively undesirable is at the heart of most (if not all) conceptions of the rule of law and related concepts. This distinguishes—in an extension of Dicey’s classic exposition—the rule of law from the rule of humans, corporations, or machines. This is not to discount the possibility, of which history is

¹⁷ Note that the ‘rule of law’ argument that I am advancing here is different from the one James Grimmelman makes in his treatment of the Sealand case. There he argues that the idea of an island with extrajurisdictional sovereignty was bound to fail because its conception of the rule of law was too thin, thereby illustrating the superiority of state-backed law creation and enforcement. James Grimmelman, *Sealand, HavenCo, and the Rule of Law*, 2012 *University of Illinois Law Review* 405.

ripe with examples, of bad or unjust law. Nor is it to ignore the important insight, prominent in US legal scholarship, that law might not always be the most effective way to steer decision-making and might empower rather than constrain those who wield power. But these are ultimately not arguments against ‘law’ as such but rather important reminders to critically examine the design, operation, and effects of any law (including global cyber-law) in action.

The idea that ‘law’ might be the solution to *any*, let alone the most fundamental Internet governance problems, will seem non-sensical (or even heretical) to many (especially non-lawyers) engaged in Internet governance. This is part of the legacy of Barlow’s ‘declaration of the independence of cyber-space’ and its strong anti-state and anti-law narratives.¹⁸ The Internet governance community has yet to realize that there is law beyond the state outside the established categories of traditional international law. Fortunately, my project of re-constituting ‘global cyber-law’ can build on variety of partly competing, partly overlapping conceptions of ‘global law’.¹⁹ Integrative accounts that recognize that law *beyond* the state is not to be confused with law *without* the state are the most promising as ‘global cyber-law’ purports to affect the law-making of states and international organizations with relevance for the global Internet.

III. The Contours of Global Cyber-Law

What is the content of ‘global cyber-law’? Among the many theories of ‘global law’, Global Administrative Law (GAL) appears to be best suited to address the accountability gaps in Internet governance. The proponents of GAL define it as “the mechanisms, principles, practices, and supporting social understandings that promote or otherwise affect the accountability of global administrative bodies, in particular by ensuring they meet adequate standards of transparency, participation, reasoned decision, and legality, and by providing effective review of the rules and

¹⁸ John Perry Barlow, A Declaration on the Independence of Cyberspace, <https://www.eff.org/de/cyberspace-independence>.

¹⁹ Neil Walker, *Intimations of Global Law* (OUP 2015).

decisions they make.”²⁰ At the heart of this definition is the insight that global administrative bodies (with and without state involvement) have in fact emerged and that they have regulatory power whose exercise needs to be subject to some constraints. For a number of reasons, it is desirable that these constraints are rooted in ‘law’.

Internet governance institutions such as ICANN and the IETF are prime examples for such global administrative bodies. Under a conventional national law framing, ICANN, a not-for profit corporation under California law, would be governed by the state laws of California and the federal laws of the United States. But these bodies of law are ill-suited to effectively govern ICANN’s regulatory function as global administrator of the Domain Name System (DNS), a key component of the global Internet infrastructure. Its global relevance and power corresponds with heightened and increasingly global demand for stakeholder involvement and accountability. After a series of governance reforms, ICANN – while retaining the legal form and organs of a not-for-profit corporation under California law – now features a highly complex decision-making and accountability structure that conforms to the GAL principles of transparency, participation, reason-giving and review. By increased GAL-compliance ICANN has alleviated persistent legitimacy concerns in the Internet governance community while putting pressure on states to conform to the same principles to the extent to which they are involved in ICANN decision-making.²¹

The IETF is an even more extreme case as it deliberately sheds established legal forms. But its decision-making can and should nonetheless be recognized as an exercise of regulatory power that incurs the need to comply with basic GAL principles. Those principles are not uniform and can and should be adjusted to the particular mission, capacity, and relevance of a particular Internet governance institution. But instead of hiding behind the veil of technical expertise, the IETF should endorse IETF-specific GAL-compliance as foundation for its decision-making.

²⁰ Benedict Kingsbury, Nico Krisch & Richard B. Stewart ‘The Emergence of Global Administrative Law’ 68 *Law & Contemporary Problems* 15 (2005).

²¹ Bruno Carotti & Thomas Streinz, *Global Internet Governance: The Internet Corporation for Assigned Names and Numbers (ICANN)*, in: Benedict Kingsbury and Richard B. Stewart, *Global Hybrid and Private Governance* (OUP 2018, forthcoming) (on file with author).

In some sense, ICANN and the IETF are the easy cases—at least through a GAL lens. Contrasting GAL with the competing concept of ‘international public law’ (as opposed to public international law) shows its superiority for the purposes of Internet governance. International public law seeks to respond (only) to the ‘exercise of international public authority’ (IPA) but its definition remains formalistic. According to von Bogdandy et al, “[w]hether an act amounts to an exercise of international public authority, in contrast to domestic or supranational authority, depends on the provision it invokes as a legal basis.”²² This understanding, while providing a clear rule to shed the national from the international, grossly miss-categorizes global institutions of internet governance. ICANN would be exercising *national* public authority despite its global reach. The IETF, which operates without any formal legal basis, would fall completely through the grid. ICANN and IETF also fail to meet the two other IPA criteria—‘publicness’ and ‘authority’. Even though both institutions claim to act in the public interest, this claim is not backed by a specific ‘mandate’ and hence not ‘public’. And even though both institutions wield significant power, this power is not grounded in international law and hence comes without a claim to ‘authority’. In sum, if asked for input on global cyber-law, international public law too often responds with a 404 error.

The harder question is whether a GAL-based account of global cyber-law can also address the problems of jurisdictional coordination between states and the role of global platform corporations. The answer to both is yes, but subject to qualifications.

There is no conceptual reason why states, acting through different agents depending on their institutional and political configuration, could not be seen as global administrative bodies themselves. To the extent that states legislate, regulate, or adjudicate Internet usage with effects beyond their jurisdiction, their formally internal law-making and/or -enforcement affects the Internet as a (potential) global public good which should trigger at least some procedural and substantive legal

²² Armin von Bogdandy, Matthias Goldmann & Ingo Venzke, ‘From Public International to International Public Law: Translating World Public Opinion into International Public Authority’, Max Planck Institute for Comparative Public Law & International Law (MPIL) Research Paper No. 2016-02 (February 25, 2016), available at SSRN: <https://ssrn.com/abstract=2770639>.

constraints. This means, in practice, that Internet law-making and -enforcement by states might have to be somewhat more transparent, participatory, and well-reasoned than the regulation of purely internal matters. It might also need to take into account human rights considerations (such as access to information), distributive impacts, as well as the eventual systematic implications of the measure on the global Internet. States, while generally maintaining that their law- and decision-making conforms to established jurisdictional categories, seem to recognize increasingly that they cannot escape the fact that the Internet has vastly expanded the extent to which seemingly domestic regulation can have extraterritorial effects. This is true for the EU's legislative process that led to the adoption of the General Data Protection Regulation (GDPR), which involved a significant number of global stakeholders. Similarly, the debate in the US Congress on the US Cloud Act also considered the impacts of this piece of domestic Internet regulation on other states (but not on other Internet governance stakeholders) and how they might respond. Under global cyber-law, national and international courts will have to be aware of their systemic role in global Internet governance as well [to be expanded]. [Discuss conflict of laws type solutions to jurisdictional conflicts and extraterritoriality]

Similarly, under global cyber-law, global internet corporations will need to accept that their freedom to operate will be constrained not just by domestic law but also by globally applicable rules whenever their decisions have a significant cross-jurisdictional impact on the Internet. Eventually, they are likely to embrace global cyber-law as a tool to enhance their legitimacy and to push-back against unwanted domestic regulation with extraterritorial effects that impede their transnational platforms and products. Global cyber-law is not necessarily an anti-corporate enterprise. In fact, there is a risk, recognized by critical GAL scholars, that an expansion of procedural requirements will only favor those who have the capacity and expertise to use these procedures. This critique has some merit but the right response is to counter-balance the power asymmetries instead of capitulating in the face of them by refraining to demand appropriate procedural requirements in the first place. In this context, it is important to recognize that one of the key features of global cyber-law is that its expansive scope allows for new and different coalitions of stakeholders who will be able to advance their interests and to express their arguments in the language of law (rather than money or raw power).

There are three additional standard critiques of GAL to which global cyber-law has to respond: the fig leaf charge, the Western neo-imperialism allegation, and a deficit of substance whose flipside is an over-reliance on procedure.

The fig leaf charge contends that GAL-type procedures tend to legitimize an exercise of power which might not be justified in the first place and should be openly challenged instead of implicitly accepted. There is some truth to this but it is hard to see how to change the power structures in Internet governance in any systemic way. In fact, introducing GAL-type procedures as global cyber-law might be more transformative than in other contexts with different baselines.

The related allegation that sees GAL essentially as novel form of Western legal neo-imperialism by which principles of US administrative law are being scaled globally, again, has a point in recognizing that US-administrative law roots in GAL are clearly visible and in pointing out that many global administrative bodies tend to be based or have been founded in the West. But, there is no reason to think that global governance and GAL have to be that way. Indeed, if GAL is to serve as conceptual foundation for a truly global cyber-law, it will need to adapt to an Internet environment in which most Internet users live in Asia and in which China's digital economic and political power is clearly on the rise.

It is true that GAL tends to rely on procedures rather than on prescribing or even openly pursuing certain substantive outcomes. This might come at the cost of over-bureaucratization at the expense of only shallow normative commitments. But it also allows for some commonality of practices when consensus on substance is yet impossible to achieve. This is exactly the situation in Internet governance. However, global cyber-law might need to contain an explicit normative commitment to the openness and globality of the Internet. After all, what makes this variant of global law 'cyber' (and different from GAL) is its explicit aim to (more or less skillfully) steer the decision-making of key actors in Internet governance to maintain the Internet as a (potential) global public good.

IV. The Normativity of Global Cyber-Law

To even raise the question whether global cyber-law is indeed ‘law’ leads inevitably into a legal theory thicket. Yet, the question seems unavoidable, because my argument for global cyber-law relies crucially on rule of law functions that allegedly only ‘law’ can provide. To point out that global cyber-law can rely to some extent on existing domestic and international legal structures whose legal pedigree is beyond doubt, does not answer the question whether the whole enterprise can claim to be ‘law’. In the discourse about the concept of law in GAL, Benedict Kingsbury has tried to advocate for a ‘social fact’ conception of law in the Hartian tradition that emphasizes sources and recognition criteria to which he adds the additional requirement of ‘publicness’ as an immanent feature of global public law / law in global governance.²³ His critics saw this as a futile attempt to preempt the charge that GAL was in fact an enterprise of natural law.²⁴

Against this backdrop, I would argue that global cyber-law has a better shot at being recognized as ‘law’ than any alternative conception of legalized global Internet governance. My optimism rests on two reasons:

The first is that the alternatives such as a universalist completely UN-led Internet governance regime are politically entirely unrealistic. In contrast, global cyber-law is not in need of a celebrated founding moment in which all relevant stakeholders endorse a certain conception of Internet governance and law. Global cyber-law, as proposed here, can develop over time as Internet governance evolves and its normative force can be recognized gradually and does not need to be recognized instantly or uniformly.

The second is the inevitability of externalities that animates the project of global cyber-law even more significantly than related projects in other areas of global governance and law. In his seminal work on ‘sovereigns as trustees of humanity’, Eyal Benvenisti develops the powerful image of the world as an apartment building in which the inhabiting states must no longer ignore the externalities they place on others.²⁵ The Internet is not only a key reason why we now live in that apartment

²³ Benedict Kingsbury, *The Concept of ‘Law’ in Global Administrative Law*, 20 EJIL 23 (2009).

²⁴ Alexander Somek, *The Concept of ‘Law’ in Global Administrative Law: A Reply to Benedict Kingsbury*, 20 EJIL 985 (2009).

²⁵ Eyal Benvenisti, *Sovereigns as Trustees of Humanity: On the Accountability of States to Foreign Stakeholders*, 107 American Journal of International Law 295 (2013).

building. Internet governance is a prime example for decision-making whose effects are significant and often not jurisdictionally confined. This is true for ICANN's decision whether or not to award .AMAZON to Amazon, Inc. (impacting the ability of everyone else, including states, to control this domain); the IETF's development of the Internet Protocols (affecting every Internet user); the EU's adoption of the GDPR (affecting anyone who uses a product that has been geared to the European market) etc. At some admittedly hard to define point, the inevitability of externalities will be the driving force behind the recognition of global cyber-law as the only legal mechanism to coordinate Internet governance effectively.

Even if recognized as 'law', global cyber-law will always straddle the law and policy frontier as well as the law and technology frontier. But its focus on rules about rule-making allows for a significantly clear distinction between the outcome of Internet governance processes (which may or may not be law, code, or whatever) and the process that leads to this outcome for which 'global cyber-law' can provide predictability, rationality, and ultimately legitimacy.

V. Conclusion and Outlook

This short paper has sketched the need, contours, and legal nature of 'global cyber-law'. My hope is that re-constituting global cyber-law in this way may not only improve global Internet governance. It may also hold valuable lessons for theories of 'global law' more broadly. 'Global cyber-law' shows how law beyond the nation state and beyond categories of traditional international law evolves and why it matters. As the Internet's importance as global information exchange infrastructure will only continue to grow, so will the relevance of 'global cyber-law'. Future research could apply 'global cyber-law' to blockchain governance which shares some similarity due to the systemic tension between distributed networking and centralized forms of legal power and control. Another question is how law's normativity can be replicated in and effectuated by technology, incorporating 'law' into 'code' in a literal sense (instead of just mandating that the code has to produce certain outcomes or has to comply with certain standards). Global cyber-law remains work in progress.