

Freedom of Expression in Distributed Networks

Ejvind Hansen

Danish School of Media and Journalism, Århus, Denmark, eh@dmjx.dk

Abstract: This paper proposes the following question: Is it possible to transfer human rights like the freedom of expression – or at least to preserve the formal protections guarding speech acts from arbitrary suppression – in a post-national setting? The question arises as an urgent matter in the context of our global system of connected markets and distributed telecommunications networks – the Internet – since, as many academics and policy makers have noted, the two tend to undermine national boundaries, putting into question the power of individual states to continue function as the traditional legal and identity-generating entities of last resort.

If this analysis is reliable the dialectical union between the autonomous individual citizen and the legally regulated nation state is broken. In this paper I will draw the consequences of that supposed break, exploring the question of the extent to which it makes sense to accord “rights” – freedom of expression – to entities that are not classical autonomous humans, and to confer them by entities that no longer bear the marks of nation-state sovereignty. The question thus is: Is it possible to transfer the normative approach of the classic liberal nation states into a global system?

The paper explores this question through an elaboration of problems for the preservation of the human right to freedom of expression: On the one hand communication on the Internet is regulated by an immense legal body, but on the other hand, the machinery for enforcement controlled by this legal body is dependent on various agencies that don't necessarily recognize its legitimacy. I will then explore whether a more technologically oriented approach could be a more fruitful approach in defining the actual limitations to freedom of expression in the new global system. My answer is that ultimately the control paradigm fails, because it is too clumsy at incorporating self-correcting measures. Thirdly, I suggest that the best solution to the challenges to freedom of expression in the global system must be a Global Government of the Internet, a government that is defined by democratic elections, a constitutional body, and deliberative institutions

Keywords: Freedom of Expression, Internet Governance, Nation State, Disciplinary Approach, Control Approach, Deliberation

Acknowledgement: This paper was presented at the 4th ICTs and Society Conference "Critique, Democracy, and Philosophy in 21st Century Information Society" at Uppsala University, Sweden, May 2012.

This paper proposes an analysis of a fundamental question in legal philosophy: Is it possible to transfer human rights like the freedom of expression – or at least to preserve the formal protections guarding speech acts from arbitrary suppression – in a post-national setting? The question arises as an urgent matter in the context of our global system of connected markets and distributed telecommunications networks – the Internet – since, as many academics and policy makers have noted, the two tend to undermine national boundaries, putting into question the power of individual states to continue function as the traditional legal and identity-generating entities of last resort.

Ideas and doctrines of human rights were articulated in close proximity with the creation of democratically founded nation states. Democratic governance theoretically depends on the idea that human subjects are autonomous, self-legislating individuals. The proclamation of human rights contained in many constitutions or codes of law were meant to protect the autonomous individual against the powers of the legislators, bureaucrats and executors who represent the state (on the emergence and ideas behind the human rights and the freedom of expression, see Joas 2011; Sunstein 1993; Jørgensen 2011).

This complex of notions (democratic governance, the distinct and independent state, and the distinct and independent subject) has been under attack, according to analysts like Foucault and Hardt/Negri, as the historical circumstances that gave birth to them have shifted. The enlightened definition of the individual subject as a rational, coherent and disciplined agent (as opposed to, say, the agent of madness, ruptures, and desire) seems to have increasingly lost its pertinence as systems of production and communication embedded within it has transformed (Foucault 1997; 2004a; 2004b; Hardt and Negri 2000; 2004; 2009). In the works of Hardt and Negri the distributed networks of the market and the Internet are pointed out as the main reasons for this change: on the one hand because new global economic agents undermine the centralised (economic and thus political) powers of the nation state; on the other hand, because the possibility of peer-to-peer and

group communicative exchanges through the Internet undermine the nation state as the prime orientation of identity formation (Hardt and Negri 2000, xi-xii).

If this analysis is reliable the dialectical union between the autonomous individual citizen and the legally regulated nation state is broken. In this paper I will draw the consequences of that supposed break, exploring the question of the extent to which it makes sense to accord “rights” – freedom of expression – to entities that are not classical autonomous humans, and to confer them by entities that no longer bear the marks of nation-state sovereignty.

Analysts like A.R. Galloway have suggested that regulation in distributed networks tends to mirror the dissolution of the Foucaultian disciplinary paradigm (as the crucial component of that paradigm, the legislative centre, weakens) in favour of control-oriented paradigms (in which regulation comes about through technical limitations of an empirical or designed nature (for instance, in encryption) in the protocols of exchange). L. Lessig has, however, problematized this, by pointing out that this is democratically problematic, because it deludes how new means of control, as for instance creating architectures that are intended to regulate use, distribution, and the like, are products of political decisions, and thus the political responsibility is blurred (Lessig 2006, ch. 7).

The question thus is: Is it possible to transfer the normative approach of the classic liberal nation states into a global system?

I will answer this question through three steps: First I will concretise reasons why the prevailing challenges of the nation states also challenges the human right to freedom of expression: On the one hand communication on the Internet is regulated by an immense legal body, but on the other hand, the machinery for enforcement controlled by this legal body is dependent on various agencies that don't necessarily recognize its legitimacy Secondly, I will more fully outline the control-oriented approach to understanding governance and present the case of its advocates, who say that it could be a more fruitful approach in defining the actual limitations to freedom of expression in the new global system. My answer is that ultimately the control paradigm fails, because it is too clumsy at incorporating self-correcting measures. Thirdly, I will suggest that the best solution to the challenges to freedom of expression in the global system must be a Global Government of the Internet, a government that is defined by democratic elections, a constitutional body, and deliberative institutions. In the fourth section I will consider the objections that have been raised against similar suggestions, and that possibly could be raised against my own: How is this suggestion going to pass muster with a U.S. government that is extremely wary of global governance, and extremely aggressive about extending U.S. law in all manners concerning the Internet? How are we going to attach an enforcement mechanism to the global government of the Internet? Lastly, what relationship should exist between the global governance of the Internet and expressions that happen behind the walls of closed communities? In my fifth and final section, I will summarise the findings of the paper.

1. Freedom of Expression with the Internet

The notion of human rights is complex. On the one hand it is a political notion; the notion of human rights is the idea across any politically defined differences and regulations, humans as humans have certain rights, certain limitations of human lives can never be legally, politically or perhaps even morally defended, certain possibilities should always be supported. Secondly, it is a legally concretized notion. Rules and laws define the concrete shapes and limits of human rights. Thirdly, the notion of human rights is also in a certain sense a practice. In order for citizens to *have* human rights, it is not enough that political ideals and legal bodies subscribe to notions of human rights. The political ideals and legal bodies should also, as it were, interact fruitfully with a practical reality; to have human rights, the ideals and rules should have a concrete impact on practice.

The relationship between these three constituting elements should be thought in tensed dialectical terms: The ideals and rules are products of theoretical reflections upon prevailing practical realities (Joas 2011; Sunstein 1993), on the other hand the notion of the human rights would not make much sense if they were simply to adapt to any reality. This normative inertia stems from the reflective abstractions that are contained in the normative bodies (the theories and the rules). These abstractions point out certain *essential* aspects of humanity. The genealogical analyses of Foucault (certainly inspired by Nietzsche – e.g. in Nietzsche 1874/1988, 248-257) demonstrate, however, that these essential aspects of humanity are products of power-struggles in concrete social practices (e.g. in Foucault 1966; 1975).

In order to make the discussion more concrete I will contemplate the example of freedom of expression on the Internet. Freedom of expression arose as a demand in the early modern period, in tandem with the emergence of the first technologies of mass-media, the printed press. The old copyist distribution of text and visual images was replaced, in this technological leap, with a few-to-

many media, which made it possible to communicate within extended political publics, while, on the other hand, giving an impetus for populations to learn to read. The government response (by states ranging from autocratic monarchies to city state republics) was to try to exert control over the content of the few-to-many structure through censorship, which operated at various levels (direct censorship, licensing of presses, taxes to raise the price of printed materials, etc.). These forms of intervention were later used with radio and television, which created a whole new awareness of space (the space of wave frequencies) and a government response claiming the majority of that space (and thus licensing out the space to broadcasters). It was technologically feasible to control communicative contributions to the public sphere except on the margins because the entry points to the public sphere were few. Most often, those entry points were situated within the jurisdiction of some prevailing political unit.

The countervailing power of democratic pressure groups rallied around the slogan, freedom of expression, firstly to counteract censorship of political speech in a balanced way. It is important to notice that these groups never succeeded in abolishing all censorship, nor for the most part did they want to. The freedom of expression is never absolute. Both the potential censors and the advocates of freedom of speech agree that in certain circumstances, and with certain types of speech, freedom of expression should be limited. Limits are often placed on (e.g.) libel and slander, morally 'corrupting' material (such as child pornography), incitement to crime, the invasion of privacy, some kinds of commercial speech, distribution of copyright protected information, speech threatening national security or military secrets, etc. (La Rue 2011, §24-25, 27).

This history points to the dialectical complexity of freedom of expression: it is theoretically necessary that democratic states preserve freedom of expression due to the nature of democracy. The freedom ensures that every citizen can act as a deserving, autonomous individual, whose contributions to the national community is theoretically considered to be of decisive importance, at least in as much as it attaches the individual to the state. On the other, however, certain kinds of expression could actually undermine the ability of citizens to exercise their rights, in as much as unlimited expression could undermine their dignity, security, self-esteem, moral character, or ability to access true information, etc. So, just as the freedom of expression facilitates democracy, freedom without state backed limitations could undermine democracy. The freedom of expression, under this reading, needs to be limited in certain ways.

Traditionally representatives of the nation state exercised the administration of this limited censoring power. The emergence of the Internet, however, produced a quantitative change in the number of entry points to the sphere of highly distributed expression such that it changed the qualitative reach of the state to limit communicative expressions. The nation state has lost its complete control as the administrator of the freedom of expression. I will reflect upon two changes¹.

1.1. Legal Regulations across National Borders

Technically it has become much more complex to censor the communicative sources. This technical enlargement of the global population's communicative potential and reach is due, in part, to the fact that the structure of the Internet transgresses the political horizon of the national state. The protocols of the Internet mirror only to a very minimal degree the national settings (with the DNS-protocol as the main exception).

However, this change in the physical communicative infrastructure has not generated an adaptation of the legal frame that still guides governance in the nation states, with each state continuing to maintain its own particular set of rules. Expressions on the Internet are thus subject to the legal rules of the states in which they are accessed by end users. Thus an Internet auction in which Nazi paraphernalia was featured may be condemned as illegal by a French court even though the auction is hosted in countries in which there is no law against it (Lessig 2006, 294-295), just as United States copyright holders may charge a Canadian site streaming television with copyright infringement according to the laws of the United States (Lessig 2006, 295-296).²

1.2. The Erosion of Limitations of Freedom of Expression

Yet these national legal moves are made in a system in which the possibility of *enforcing* sentences that condemn expression is difficult to arrange. In some well publicized cases, national jurisdictions have succeeded in closing down Internet-mediated sites, most recently in the case of Megaupload.com. Cases like Wikileaks, Openleaks and The Pirate Bay, however, demonstrate that

¹ The original development of the following argument was published in Hansen 2011a.

² See Brownsword 2008, 197-201 for further examples.

this is not always possible even for a transnational power like the United States. By placing the content of the sites on servers placed in expression liberal countries with no clear exchange agreements, it is possible to distribute information that would otherwise be kept hidden.

Wikileaks explicitly declares that the fight against expressive limitations is incorporated in their main mission:

“WikiLeaks has sustained and triumphed against legal and political attacks designed to silence our publishing organisation, our journalists and our anonymous sources” (Anonymous 2011).

The result of 1.1 and 1.2 is that the prevailing limitation of the freedom of expression is unsettled. To take a well known political example: Is it allowed for Nazis to deny Holocaust? In post World War II Europe, this kind of activity was banned; in the US, the right to Holocaust denial is protected. Thus, the situation emerges where Nazi web pages are (at the outset) available in both the U.S. and the restrictive European countries, much as Nazi printed material would be available to a European traveller who came to the United States. So, who has the final say on the licitness of these Nazi web pages? And by what means can restrictive countries enforce their laws upon the infringing websites?

On the one hand (1.1) our contributions to the Internet are thus potentially subject to any limitation articulated in the laws in every nation state. On the other hand (1.2) with some effort it is possible to ignore these restrictions because Internet sites, hosted in countries without these limitations, are accessible to citizens of restrictive nations without the latter being able to shut down the source. The actual power of mechanism 1.1 and 1.2 to a large extent depends on the eagerness of the prosecutors, which in turn respond to the larger arrangement of geo-political power. If you as a Swede express libellous views on some provost in a Scottish city, the likelihood of being prosecuted is considerably less than if you publish confidential diplomatic correspondences of the United States.

In as much as the limitation of a right has two aspects (de jure and de facto), the limitation on freedom of expression on the Internet is still unfocused. As a communicative agent on the Internet you cannot know in advance whether or not your statements will get you in legal trouble somewhere in the world where you can be accessed – unless you are acquainted with the laws of any nation state in the world and the interests of powerful agents. However, a human right that becomes this unstable loses its status as a human right. The dialectical relationship between ideals, rules and practices loses its impetus if it becomes unclear which rules apply to which practices. The human right to freedom of expression loses its function, which is to protect your expression.

2. Alternative Strategies for Defining the Freedom of Expression

The failure of the WGIG is emblematic of the crisis in the traditional disciplinary paradigm that conditioned the birth and development of the legal bodies devised for governing nation states. If human rights like the freedom of expression are bound to this disciplinary paradigm, then its destruction would seem to doom human rights discourse – one would have to talk, instead, in a different way about rights in the new global paradigm. In fact, theorists like Foucault, Hardt and Negri and Lessig have argued that the traditional law-based form of governance (in which each individual is disciplined to act according to the norms of the common good) is gradually replaced by a regulative approach (which dispenses with the appeal to normality and appeals, instead, to equilibriums). Instead of focussing upon the individual and her body, the individual is deemed unpredictable and hence focus becomes statistic-based regulation of the population (Foucault 1997, 218-219; Foucault 2004, ch. 4).

Since, as argued in the previous section, an unregulated freedom of expression is not desirable, the question arises whether the regulative approach can replace the disciplinary in this field. A. Galloway argues, in *Protocol: How Control Exists After Decentralization*, that this development can be seen in the protocol-based regulations that happen on the Internet. According to this interpretation, regulation on the Internet does not happen through centralised normative rules about what is allowed. Regulation is peer-centric, a spontaneous order arising from the fact that entrance into the Internet is a matter of adhering to certain instrumental protocols – such as those regulating (a) physical layers (the physical links between the communicating hosts), the (b) Internet layers (IP –

how to get to a specified addressee), the (c) Transport layers (e.g. TCP, UDP, RTP), and the (d) Application layers (e.g. FTP, HTTP, SMTP).³

This raises the question whether it is possible to preserve the social space for human rights carved out by the disciplinary regime within regulative or control regime, embodied in the distributed protocol structures of technological designs (Brownsword 2008, ch. 5). Lessig makes the case that the latter blurs the responsibility of existing power structures in as much as that responsibility is indefinitely differed by the architecture of the system (Lessig 2006, 133-135). According to Lessig it is important that we know who to criticise if existing power structures produce problems. This argument, however, presupposes that governance in the disciplinary system was wholly identical with clearly responsible politicians. But it is not at all clear that the system of policymaking has ever worked this way. Nor does this give us guidance for the present case, in which nationally embedded politicians, as demonstrated in the previous section, tend to lose their ability to actually impose lawbased regulations in the existing flows of communication. In the latter case, would a protocol based alternative then be our preferred, or even inevitable, option?

In its present form, the Internet is clearly overdetermined by a mixed regimes of disciplinary (nationally led) and control (transnational and architectural) factors. If the former were to evaporate, it is easy to envision the Internet becoming an informational wild west of identity theft, misinformation, threats, personal attacks, and jammings that would quickly turn the Internet into an unprofitable, or at least highly risky, venture. In its present shape the Internet preserves a broad latitude for users to engage in certain kinds of “bad behaviours” or at least behaviours outside the norm without this latitude interfering with other behaviours on the net – much as civil life allows for people to behave in all kinds of unethical ways (lying, for instance) without requiring the intervention of the police. But that broad latitude is conditioned, in part, because there is a community wide assumption that real harm to other communicative and social agents does bring punishment in the offline world, if the perpetrator is discovered.

Of course, there have been proposals to diminish the need for off-line intervention by employing protocol-based solutions to “bad behaviour”. For instance, it has been proposed that a more responsible approach to the distribution of information on the Internet would be to link all information to the physical (off-line) identities of those who distribute it, abolishing the ability to be anonymous on the Internet.

The advantage of abolishing anonymity is that it would become possible to hold the distributors responsible. If this change was paired with a rating system in which it was made possible to rate the trustworthiness of the distributor, this could become an indicator of how trustworthy the received information is. Such rating systems are already at play in various existing communities (Benkler 2006, 75-80). The drawback of current systems is, however, that it is too easy to change your identity if it becomes too disreputable. Due to the potentially infinite entrance points into the Internet (which is a key feature of the system) it is easy to change your identity. If, however, physical identities were introduced in the core TCP/IP-protocol (so in order to distribute information, your digital name will be attached to it), then identity change could be made more difficult.⁴ This will certainly not guarantee that no harmful information (such as uncontrolled dissent against corporations, governments, or powerful organisations, libel, breaches of privacy, etc.) is distributed. It will, however, conform to the control-paradigm of governance, which is that *statistically* people will feel more afraid to act in ‘disreputable’ ways. *Ceteris paribus* information on the Internet would thus become more respectful. And in cases where (unnecessarily) harmful information is distributed, it will become possible to rate the distributor (and thus the information distributed by him/her) as not trustworthy.

However, there are also some disadvantages to this approach. At least two come to mind: (i) on the one hand this change of protocols would be a strong tool for surveillance strategies. If every virtual step is marked with a clear identity-stamp, it would become easy to store this information about our activities, linking them together across various sites, and before you know it, advanced commercial and governmental agencies will know more about you than you do yourself.⁵

³ This division in four layers was presented in Postel 1981. One could supplement it with an analysis of (less formal) protocols that regulate which kinds of social behaviour in the communities is conceived of as appropriate and comprehensible (Galloway, 39-41, 129-130).

⁴ In recent years Facebook has been successful in creating a solid link between the virtual and physical identities of people. In many discussion communities this link is being used to make certain that the discussions do not deteriorate, because people have to login with their Facebook account, and their contributions will be linked with this semi-physical identity. People are thus less inclined to be too brutal in their opinions. On the other hand, this trend certainly also carries the risk that people become too cautious about what they post – thus leading to less feedback, perhaps less creativity, etc.

⁵ For an elaboration on the use of surveillance techniques on the Internet, see Andrejevic 2007.

The second disadvantage is that (ii) it would disarm an important critical resource that has been part of the Internet legacy: The ability of citizens to leak information and coordinate subversive activities (an ability that is decisive especially in totalitarian regimes).

The latter objection points to the heart of a general problem with pure control-based approaches to governance: Sometimes we need the possibility of breaking with existing laws and rules – if the laws and rules are unjust.⁶ We thus need a space in which we have unhindered and continuous ability to contemplate the existing rules and laws and to adjust the rules if necessary.

Even though it may be thinkable to create a regulative control-system that could counteract some of the unhappy aspects of the Internet, it would always be vulnerable to two objections: the old objection of who will guard the guardians, first raised against Plato's ideal Republic; and secondly, the objection of unforeseen negative consequences of interfering with the flow of information, considering that anonymity (or pseudonymity) itself is an information marker. Any regulative social system (whether law- or technologically based) should be open to self-reflection and self-adjustment.

3. The Global Government of the Internet

Our tentative conclusion so far is that it is feasible to create changes in Internet protocols to re-structure the end-user experience. And given this factor, we might be able to facilitate social relations with an arguable balance between freedom of speech protection and communication harms generated by breaches of truthfulness and fairness. But just as our survey of UN approaches to global communication governance failed to overcome obstacles associated with national interests, so, too, our brief consideration of banning anonymity shows that changes to meet governance problems on the level of technical engineering do not deal with the level of the problem we started out with: who should *decide* the actual shape of the socio-technical structures? Who should be held responsible if they fail, and who has the right to adjust the settings if unforeseen problems arise?

These questions raise a point put forward by G. Agamben in his *Homo Sacer*: social systems will tend to become monopolized by a small ruling elite unless they have a robust relationship with outsiders – unless they allow outsiders 'inside'. Social systems introduce various kinds of order and predictability into social relations – some aspects of the world are accentuated as significant or important –and their survival depends on whether their participating agents find the order and predictability beneficial (on individual and community levels) and fruitful. At the same time, however, the trade-off to ordering and normalizing certain views and routines is that other views and ways of doing things are marginalized or negated. This may be a matter of the generally agreed sense of what is important in this world, which delegitimizes what is not considered important. But there is also a cost to the success of this process, as consensus complexes of views and ways of doing things, if unchallenged by alternatives, tend to an inertial conservatism, leaving them vulnerable to uncontrollable and unexpected changes in the environment. Thus, for a system to incorporate maximum adaptability, it must be able to incorporate the challenge of the stranger – tolerate it, understand it, respond to it, change itself in relation to the strength of that challenge. This is a lesson that a prevailing system that gains hegemonic impact, such as the Internet, must take seriously.

The question in terms of governance becomes the following: if the inherent limitations of the nation state (and of its international representative, the UN) are mismatched with the transnational organization and power of the Internet, is there one unique realistic counterpart that could govern it, or should that governance be fragmented and distributed? What institutions are conceivable that could have power, legitimacy, and decision-making capacity over the Internet?

The Internet at present presents us with a number of normative institutions constituted specifically to make rules for its functioning and security. Institutions like ICANN and ISOC (The Internet Society) already produce regulations and adjustments of the Internet, and ordain procedures for introducing new technologies. From a political point of view, the problem with ICAAN is on the one hand that it mainly refers to the US government. Secondly, the lack of deliberative or democratic procedures surrounding its decisions entails that the interests of the transnational Internet community is only indirectly represented, there. ISOC, being relatively open, community based, and having a record of decision-making participation in developing the Internet, might be a more obvious candidate. However, even though it is a composite organisation without national or international ties, and with an extensive membership base, it still lacks the political *legitimacy* that follows from real democratic procedures. In its present form, ISOC is best understood as a NGO.

⁶ This point is forcefully articulated in J. Derrida's *Force de loi* (1994).

Hardt and Negri have convincingly argued that NGO's paradigmatically embody the restructuring of power that comes with the fall of the nation state and the emergence of Empire (Hardt and Negri 2000, 35-38, 312-314). They define the term NGO in the following way:

"any organization that purports to represent the People and operate in its interest, separate from (and often against) the structures of the state" (Hardt and Negri 2000, 312).

While Hardt and Negri show that the claim that NGO's represent the people is baseless, they do acknowledge that NGOs may find legitimate roles in articulating the voices of those outside the small circle of the policy makers and the corporate and political elite. But as one would expect, in a political system in which the most powerful have the most resources, the strongest NGOs, the best resourced, most publicized, and most influential, are often those who simply re-articulate the voices of the most powerful interests in society. As such NGO's often tend to serve the most conservative interests.

If by some unlooked for circumstance, ISOC took over the role of governing the Internet – which one assumes would give power to certain voices of the Internet community that are normally "outside" the decision-making sphere – it would thus be necessary for it to transform its NGO-role to a governmental one, with a more clearly defined democratic mechanism. This would require at least three changes: the present procedures of decision would have to be supplemented with democratic elections; a democratic constitution would have to be created, articulating the procedures and rules governing the processes of decision; deliberative institutions and -procedures would also have to be created, making certain that decisions are not only based on arbitrary power plays.

3.1. Democratic Elections

Having democratic elections is well within the reach of any Internet organization. The main challenge to such a global process would be similar to the challenge of any election, on a much more massive scale. Thus, one would want to ensure that each person only had one vote, and that the personal choice of each citizen was protected from external coercion. As to the former challenge, technologies of digital signatures that identify uniquely the physical identity of the users have already been developed, and these could be used in this case. The latter challenge has a more difficult geo-political component. If elections in the national space of numerous countries are exercises in coercion (Iran, Syria and Azerbaijan, for example), then how could the Internet users in these polities freely exercise their voting rights in an Internet election? Especially as the use of digital identification equipment, if it fell into the hands of the government, would make it dangerous to vote against the wishes of the ruling party. One way to minimize this problem would be to make certain that the elections are held secret. In order to insure this it will, however, probably be necessary also to establish institutions for independent election monitoring, making certain that there are no physical surveillance over the voting act.

3.2. Constitutional Body

If the problems of elementary voting procedure are solved, there remains the problem of the first global democratic constitution. The constitution is a performative document that, by its defining nature, inscribes into the organization the parameters under which it will operate. In this case, one requires clear definitions of jurisdiction, the legitimate aim and scope supervening on any possible regulation, and the codification of transparent procedures leading to decision making under these rules – as well as a way of amending them.

These formal questions are matched with substantial and specific ones: who exactly will write the constitution? How will these writers find backing? And how, finally, without any physical force of their own, will they persuade nation states to cede power to a transnational entity representative of the global population of Internet users, not national citizens? At present, they apparently are not willing to so (cf. the WGIG discussion in 2005, mentioned above).

As argued in section I, the current structure in which nation states seek to maintain legal regulations that only to some extent can be enforced, is not a helpful starting point for the maintenance of the Freedom of Expression. Nation states are decreasingly able to enforce their legal bodies, and at some point it will probably become more attractive to subscribe to common rules that can be enforced, rather than maintaining nation specific rules that cannot. This will probably not be acknowledged synchronically all over the world. It is easy to envision the creation of the constitution starting as a regionally limited project, being open for new nations to join when they find it convenient and thus creating a slowly intensifying pressure on other nation states seeking to retain control of this space. The beginning will probably not promise any transformative gains, simply because

the limited regional reach will still be comparable with the reach of the nation states. However, this will mainly have to be a problem in relation to the need to limit the freedom of expression, since the included nations can agree not to extradite citizens to countries that have not signed the constitution.

So, even though very restrictive countries might not feel any urgency in transferring their powers to the global government of the Internet (because, for instance, they fear any kind of loss of control over their citizens), this would not necessarily undermine the work of the global governing body. The Internet citizens existing outside of the restrictive Internet spaces would not have to worry about adhering to the norms and laws of the latter.

As to the consensual limits of freedom of expression (in order to secure privacy, security; to avoid distribution of (e.g.) child pornography, etc.), there will surely be pirate areas, as there are now. These pirate areas now are not encouraged by nation states, but, on the contrary, by the lack of nation state power. They pop up in vacuums. And, just as now, pirate Internet sites clustering in weak jurisdictional areas will be cut off from the Internet system when they are found by the governing body.

For this vision to become more than a thought experiment there must be action by governments in the nation states who feel or realise the inconveniency of the prevailing state of affairs. The European Council has taken some preliminary steps in defining some principles for Internet governance that might serve as a starting point (Council of Europe 2011). In order for the global government to have real global potential it would, however, probably be important that it is not presented purely as a European project.

3.3. Deliberative Institutions

If the vision we are elaborating actually started crystallizing in reality, the challenge that would be the hardest would be making spaces for deliberative procedures in the political processes. Deliberative processes do not necessarily have to be conceived of in the Habermasian manner. Habermas' account has often been criticised as being Western-centric, and privileging a certain historically specific set of Enlightenment ideals at the expense of other cultures (e.g. in Benhabib 1992; Fraser 1993). However, the founding intuition of his notion of deliberation is that decisions should be made on the background of a reflection upon what would be best for the affected parties – rather than on the background of a balancing of differing interests. In the deliberative approach, sometimes there are interests that do not deserve to be part of the balance.

Now, it would probably not be controversial to state that the success of the nation state in securing deliberative procedures is limited. However, the national outlook leaves a room for certain complexity-reducing exclusions. In the national outlook it is possible to refer to the prevailing culture or the "our way of living". So, if you want to be a democracy subverting terrorist, you do not belong to our culture. A global government of the Internet could actually do the same thing: If you want to distribute information that is not within the Internet-definition of free expression, you cannot use the Internet. You would have to use other communicative media.

But the main problem of deliberation in a global government of the Internet remains: Which kinds of exclusions could be defended, in order for the deliberative process not to be too overwhelming?

As a starting point the answer probably could be, that no exclusions could objectively and neutrally be defended – but we still need to have exclusions.⁷ Thus the decisions of the global government ought to be as inclusive as possible. Absolute inclusion is neither possible nor desirable, but the very process of trying to deliberate the actualised exclusions will make us more aware of prevailing exclusions.

The point is that a global government of the Internet in a certain sense is obliged to respect cultures all over the world. At the same time, this is not actually possible. To take an obvious example, it is not possible both to respect children's rights to physical integrity (by the prohibition of child pornography) and paedophile desires of sexual amusement (through consumption of child pornography). This is, however, a problem with every kind of regulation. And regulation happens already. The advantage of the global government is that regulation will be based upon explicit rules – i.e. it becomes possible for adversaries to articulate their dissent, and demonstrate why the rules, according to their views, are unfruitful, unhappy or even repressive.

⁷ In Derridean terms one could call this the *aporia* of global government. At the outset, it would seem natural, given the nature of the communicative relations on the Internet, to claim that a first duty of the deliberative body of the global government of the Internet would be to make sure that interactive component is not undermined. I have, however, in previous works argued that even the notion of interactivity can be used in both democracy promoting and -undermining ways (Hansen 2010; 2011b; forthcoming).

By articulating exclusions, they become subject to discussion and debate, which would be an improvement over the present state of affairs, where exclusion is arbitrary and national.

4. Possible objections

It is certainly outside the scope of an article to exhaust the problems surrounding a global government of the Internet. Had it been that easy, it would probably have been done long time ago. The pretention of the paper is thus not to exhaust the notion of a global government of the idea, but to sketch a scenario in which it is feasible. In order to strengthen the sketch I will in this section try to contemplate some of the most pressing objections to our scenario: Why should this suggestion convince the US that it should slack off its control of the core technological resources – given earlier failings in doing the same? Which powers of enforcement should be attached to the global government of the Internet? How should we deal with expressions behind the walls of closed communities?

4.1. Convincing the US

The Internet was in many ways a creation of the United States and ICANN (who administers the Internets systems of unique identifiers and ensures its stable and secure operation); and it is still controlled by the United States. All earlier attempts to loosen this control have come to naught. The United States has always refused to transfer any powers of control – referring to worries about the efficiency of the technology and the protection of the First Amendment to the United States Constitution, in which a very “free” account of the freedom of expression is articulated.

The worries about inefficiency would, at least to some extent, be obviated by the point that the global government of the Internet does not have to reach consensus between differing countries with differing interests – as is the case in the present UN-structure. The global government of the Internet could be just as efficient in decision making as any parliament (depending certainly on the constitutional procedures). The decisions of the global government of the Internet could be just as based on expert advices as in any existing national government, and the global government of the Internet could also decide to delegate out the technical regulations over to expert based institutions – just like the administration of the United States has decided to hand over the technical regulations to ICANN.

As to the worry about the first amendment, the main counterargument would be that *with* the global government of the Internet, it becomes possible to actually prosecute court decisions. *Without* the global government of the Internet the United States may uphold an account of the freedom of expression that, at least in some ways⁸, is more liberal than many countries in the worlds, but in fact its rulings will be rendered null and void elsewhere. This is a danger in a globally connected economy, and among a globally connected citizenry.⁹

4.2. Powers of Enforcement

A second challenge for the sketched solution is how the global regulations should be enforced. Are we envisioning a global police force? A global court?

At the outset the sketched solution is indifferent as to how regulations could be enforced, since the main aim is the clear definitions of the limitations of freedom of expression. Certainly the global government will have to articulate what punishment should be affiliated with what crimes, but who should actually prosecute and enforce these decisions is not decisive. The courts and police of the nation states can enforce the law, but will probably have to be supplemented by cross-national authorities who can service the prosecution of cross-national criminality.

4.3. Regulation of Closed Communities

A third challenge relating to the regulation of communicative exchanges on the Internet is: What should we do about the criminal expressions that happen within closed communities – and thus cannot be accessed.

At the outset such exchanges are comparable with private exchanges, and to large extents they are thus no proper targets of legal regulation. However, in some cases (e.g. child pornography) there are communicative exchanges that should not even be allowed in private settings. In relation

⁸ Not, however, when it comes to the balance between freedom of expression and distribution of copyrighted intellectual property.

⁹ Demonstrated recently in the Wikileaks-case.

to such cases it will probably be necessary to articulate legal procedures for requesting private access to such sites. However, as UN Special Rapporteur Frank La Rue has emphasised, it is important that such cases are clearly defined (La Rue 2011, §§24, 32).

5. Conclusion

The overall point is that certainly a regulated Internet will and ought never evolve into an absolute open network of communication and information sharing for many reasons grounded in social practice and practical reason. The gain from the global government of the Internet is mainly that we get to *know where* the limits of our freedom of speech are – as opposed to the present state of affairs. This makes it possible for its “citizens” to be in favour or against of the prevailing limitations. And that is a good starting point for political deliberation.

One important thing to remember is, however, that the Internet has no necessary monopoly on communication. If groups find their needs violated by the global government of the Internet, they can communicate through analogue media, or they can (at least if they have the financial and technological backing) create their own alternative digital network.

Once we have in place an autonomous structure of global Internet governance, we will not bring to an end destructive communication and information-sharing; our gain rather is an addition to freedom that inheres in having a clear picture of the limits of the freedom of speech. Clear limits of human rights being an important starting point for their persistent existence, much would thus still be gained.

References

- Agamben, Giorgio. 1998. *Homo Sacer: Sovereign Power and Bare Life*. Stanford: Stanford University Press.
- Andrejevic, Mark. 2007. Surveillance in the Digital Enclosure. *The Communication Review* 10 (4): 295–317.
- Anonymous. 2011. About: What Is Wikileaks. Accessed October 4, 2012. <http://wikileaks.org/About.html>
- Benhabib, Seyla. 1992. Models of Public Space: Hannah Arendt, the Liberal Tradition, and Jürgen Habermas. In *Habermas and the Public Sphere (Studies in Contemporary German Social Thought)*, edited by Craig Calhoun, 73–98. Cambridge: MIT Press.
- Benkler, Yochai. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.
- Brown, Deborah. 2008. A Cautious Embrace of Internet Freedom at the UN Human Rights Council. *The Interdependent*, March 15, 2012. Accessed October 4, 2012. <http://theinterdependent.com/120315/a-cautious-embrace-of-internet-freedom-at-the-un-human-rights-council>
- Brownsword, Roger. 2008. *Rights, regulation, and the technological revolution*. Oxford: Oxford University Press.
- Council of Europe. 2011. Declaration by the Committee of Ministers on Internet Governance Principles, September 21, 2011. Accessed October 4, 2012. <https://wcd.coe.int/ViewDoc.jsp?id=1835773>
- Derrida, Jacques. 1994. *Force De Loi: Le 'Fondement Mystique De L'autorité'*. Paris: Galilée.
- Foucault, Michel. 1966. *Les mots et les choses: une archéologie des sciences humaines*. Paris: Gallimard.
- Foucault, Michel. 1975. *Surveiller et punir: naissance de la prison*. Paris: Gallimard.
- Foucault, Michel. 1997. *Il Faut Défendre La Société: Cours Au Collège De France, 1975-1976*. Paris: Gallimard.
- Foucault, Michel. 2004a. *Sécurité, Territoire, Population: Cours Au Collège De France 1977-1978*. Paris: Gallimard.
- Foucault, Michel. 2004b. *Naissance De La Biopolitique: Cours Au Collège De France (1978-1979)*. Paris: Gallimard.
- Fox News. 2005. Who Should Control the Internet? *Fox News*, November 10, 2005. Accessed October 4, 2012. <http://www.foxnews.com/story/0,2933,175096,00.html>
- Fraser, Nancy. 1993. Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy. In *Habermas and the Public Sphere (Studies in Contemporary German Social Thought)*, edited by Craig Calhoun, 109–142. Cambridge: MIT Press.
- Galloway, Alexander R. 2004. *Protocol: How Control Exists After Decentralization*. Cambridge: MIT Press.
- Hansen, Ejvind. 2010. Actuvirtuality in the Internet-Mediated Political Public Sphere. In *Representation and Contestation: Cultural Politics in a Political Century*, edited by Ching-Yung Lin and John McSweeney, 27–46. Amsterdam: Editions Rodopi B.V.
- Hansen, Ejvind. 2011. Grænser for Ytringsfrihed. *Journalistica - Tidsskrift for Forskning i Journalistik* 1: 92–111.
- Hansen, Ejvind. 2011. Den Dialog-udfordrende Journalist. In *Forandringens Journalistik. 40 Års Tilbageblik*, edited by Roger Buch, 97–117. Aarhus: Forlaget Ajour.
- Hansen, Ejvind. Aporias of Digital Journalism. *Journalism – Theory, Practice and Criticism* (forthcoming).
- Hardt, Michael, and Antonio Negri. 2000. *Empire*. Cambridge: Harvard University Press.
- Hardt, Michael, and Antonio Negri. 2004. *Multitude: War and Democracy in the Age of Empire*. New York: Penguin.
- Hardt, Michael, and Antonio Negri. 2009. *Commonwealth*. Cambridge: Harvard University Press.
- Joas, Hans. 2011. *Die Sakralität der Person. Eine Neue Genealogie der Menschenrechte*. Berlin: Suhrkamp.
- Jørgensen, Oluf. 2011. *Mediejura – Det Handler Om Informations- Og Ytringsfrihed*. Aarhus: Forlaget Ajour.
- La Rue, Frank. 2011. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*. UN Document A/HRC/17/27, 2011. Accessed October 4, 2012. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
- Lessig, Lawrence. 2006. *Code: Version 2.0*. New York: Basic Books.

- McCarthy, Kieren. 2005a. Bush Administration Annexes Internet. *The Register*, July 1, 2005. Accessed October 4, 2012. http://www.theregister.co.uk/2005/07/01/bush_net_policy/
- McCarthy, Kieren. 2005b. UN Outlines Future of US-less Internet. *The Register*, July 15, 2005. Accessed October 4, 2012. http://www.theregister.co.uk/2005/07/15/un_wqiq_report/
- McDowell, Robert M. 2012. The U.N. Threat to Internet Freedom. *The Wall Street Journal*, February 21, 2012. Accessed October 4, 2012. <http://online.wsj.com/article/SB10001424052970204792404577229074023195322.html>
- Nietzsche, Friedrich. 1874/1988. Unzeitgemässe Betrachtungen, zweites Stück: Vom Nutzen und Nachteil der Historie für das Leben. In *Kritische Studienausgabe 1*, edited by G. Colli and M. Montinari. Berlin: Deutscher Taschenbuch Verlag.
- NTIA. 2005. U.S. Principles on the Internet's Domain Name and Addressing System, June 30, 2005. Accessed October 4, 2012. <http://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system>
- Postel, Jonathan. 1981. Internet Protocol. *Request for Comment*, 791.
- Sunstein, Cass R. 1993. *Democracy and the Problem of Free Speech*. New York: The Free Press.
- UNHRC. 2012. Panel on Right to Freedom of Expression, 19th Session Human Rights Council, February 29, 2012. Accessed October 4, 2012. <http://www.unmultimedia.org/tv/webcast/2012/02/panel-on-right-to-freedom-of-expression-19th-session-human-rights-council.html>
- Wagner, Ben. 2011. Freedom of Expression on the Internet: Implications for Foreign Policy. In *Global Information Society Watch 2011. Internet Rights and Democratization. Focus on Freedom of Expression and Association Online*, edited by Alan Finlay, 20–22. Goa: Dog Ears Books and Printing.
- Wright, Tom. 2005. EU and U.S. Clash over Control of Net. *New York Times*, September 30, 2005. Accessed October 4, 2012. <http://www.nytimes.com/2005/09/29/business/worldbusiness/29iht-net.html>

About the Author

Ejvind Hansen

is research director at the Danish School of Media and Journalism. He is focussing on the cultural implications of digital communication. In 2005 he defended his PhD dissertation, *Embedded Critique in a Tensed World*, in which he investigates the conditions for critique in the aftermath of certain insights into the embeddedness of our practices. His work is generally situated in the field of critical- and poststructuralist theory.