Law encoded: Towards a free speech policy model based on decentralized architectures

By Argyro P. Karanasiou

Abstract

The free exchange of data between many interconnected nodes, in the absence of a central point of control, has been at the heart of the Internet's architecture since its inception. For its engineering architects "*if the Web was to be a universal resource, it had to grow in an unlimited way*", thus "*its being 'out of control' was very important*" (Berners-Lee and Fischetti, 1999). Yet, this simple deign choice has had a serious impact on conventional legal thinking. This paper highlights the importance of online decentralized architecture as the perfect substantiation of the autonomy rational underpinning the right to free speech.

In doing so the paper analyses the core principles supporting the Internet's architecture on their merit to the promote the user's autonomy and self-realisation through speech. Following the free speech rationale for autonomy, it is observed how some simple engineering decisions for an open decentralised communicatory platform can build a user-centric ecology for speech. To validate this hypothesis two main architectural choices are examined as to the potential they hold for free speech: the principles of Modularity and End-to-End (E2E).

The paper concludes that in terms of free speech, law and net architecture should be seen as complementing factors instead of opposite controlling deities. In this respect, Lessig's mantra that "*code is law*" is paraphrased to read as "*law encoded*", meaning that the law should strive to maintain the core architectural Internet values promoting human rights, and free speech in particular.

Contents

1. Prologue: On shaken trust and the online *Rechtsstaat*

A recurring theme when discussing online policy-making at a transnational level is the issue of regaining trust. Online trust has been a key term for the EU Commission's digital agenda (Kroes, 2013), while it has also been identified as one of the main priorities of the Obama administration as outlined in most of Hillary Clinton's (2011, 2010) speeches. The original disbelief of state interference in the early days of the Internet has now given way to an absolute lack of trust: this became especially evident after the Snowden revelations about the NSA surveillance tactics online (Donohue, 2013). However, this lack of trust towards online policy-making is not only evident vertically, namely between the citizen and the state; it stretches to an international level, involving state-to-state relations. For some states, Snowden offered a chance to criticise the U.S. and to some extent key points addressed in European aspects of Internet policy-making: Russia offered asylum to Snowden, China expressed fears over cyber-espionage pushing for a U.N. governance model online, while Brazil accused the U.S. of breaching international law and expressed an interest in facilitating discussions to strengthen Internet governance. Trust has also been identified as a major challenge for online policy-making by ICANN, the Internet's main governing body responsible for domain names (Chehadé, 2013). This lack of trust hardly comes as a surprise given the limited transparency and accountability of non-state actors that operate as agents indirectly implementing state control online in an opaque manner. In the aftermath of Snowden, top tech companies, such as Google, Apple, Microsoft, Yahoo!, Facebook and AOL, addressed the U.S. Senate Judiciary Committee urging for more transparency and accountability, in an attempt to regain lost trust. The same companies have however been criticised for their non-transparent configuration of their privacy settings (Edwards, 2013), their all-encompassing proprietary policies (Elkin-Koren and Salzberger, 2013) and their use of sophisticated algorithms to harness masses of data online (Mayer–Schönberger and Cukier, 2013).

The intermediation [1] of online speech no doubt holds significant ramifications for its legal protection. This has unavoidably shaken the user's trust in the legal mechanism of upholding human rights online. The new mediating forces that have joined in with the ability to control online informational flow (Cohen, 2016) are not directly bound to any constitutional obligations to uphold free speech. The Ruggie Principles [2] have created a soft law of international responsibilities for online corporations to uphold human rights online. However, these Principles cannot guarantee full protection of free speech [3]. The U.S. First Amendment appears to have been drafted with the understanding that the State is the sole source of infringements on the right to speak freely; intermediated speech is thus a challenging concept calling for a wider interpretation. In Europe, on the other hand, although freedom of expression under Article 10 of the European Convention on Human Rights is predominantly understood as a negative right, there seems to be some ground for "implied positive obligations" [4] applicable to private actors [5]. That said, with regard to the Internet, these obligations refer to access to the information online and do not include a right to impart information, nor do they touch on issues of administering the informational flow [6] or the Internet infrastructure in general.

At the same time, the current intermediary liability rules preclude any direct state action to enforce free speech online. Instead, self-regulation of intermediaries is encouraged by the "safe harbour" statutory provisions, which grant them immunity from liability for user-generated unlawful content. The EU's E-Commerce Directive [7], granting immunity to intermediaries acting as mere conduits or offering hosting and caching services online, follows the example set by similar pieces of national legislation introduced in Germany [8], France [9] and the U.K. [10]. Safe harbours are generally considered instrumental in constructing an indirect enforcement mechanism of censorship through the delegation of certain powers to private corporations paired with a limited scope of accountability [11]. At the same time, entrusting online intermediaries with the task of protecting free speech — while themselves being under no direct constitutional obligation — runs the risk of limited "substantive protection for individual rights and due process" for the users (Brown, 2013).

Transparency and accountability seem to be key concepts in enforcing the constitutional protection of human rights; they are also the driving wheel behind the Internet's growth and sustainability. However, as noted above, online intermediaries — acting either as the states' agents enforcing its policies online or out of personal interest to gain revenues — seem to be lacking in both. As a result, the constitutional protection of free speech, limited only against state arbitration, seems to be offering limited protection against the challenges posed for free expression in the digital era. What is suggested here is that the archetypal design for the Internet's infrastructure can serve as an embodiment of free speech values, enhancing the user's autonomy and promoting thereby free expression.

The next section turns to the Internet architecture for answers; it is argued that some of the core values underpinning the right for free speech are indeed visible in the engineering principles, upon which the Internet was built. In fact, it appears that the architectures of the right to free speech and the Internet share a common value underpinning both: the respect to individual autonomy. To iterate this point, the following section attempts a legal evaluation of the Internet's core architectural principles. The remainder of the paper follows a techno-legal approach to ultimately conclude that maintaining a user-centric architecture can restore the user's trust in the online *Rechtsstaat*.

2. Architecture is politics, architecture is law

In many ways, architecture is believed to have the power to instruct human behaviour. This may occur either directly or indirectly. In the case of direct intervention of architecture in human free will, one can think of the simple example of walking on a bridge as the only way to cross a river. In this example, architecture evidently guides human behaviour and limits free will to the only viable solution; the one provided by architecture. It is accepted, though, that architecture can also affect human behaviour indirectly through its communicative effects. The design of a building can either be symbolic [12] or it can convey general social values [13], ruling social behaviour in the same manner law does. For example, Foucault's (1977) reading on Bentham's panopticon demonstrates how spatial arrangements can affect human behaviour; architecture can thus be seen as an extra-regulatory force, working alongside law.

In cyberspace, architecture matters and — as will be demonstrated shortly — it has the power to frame online behaviour. This of course is hardly a new observation. Put simply by Mitch Kapor, “architecture is politics” a phrase later formalised and subsequently popularised by Lessig (2006). It is true that people tend to forget that the Internet is an artefact (Post, 2009); an artefact designed on some elementary “*architectural assumptions*”, namely its *layered structure* and the *end-to-end structural principle* that runs through its infrastructure. Their combination accounts for the Internet’s unique set-up. In a way they could be regarded as constituting the main core of the Internet’s architecture; the fundamental principles that aside from holding certain significance for its technical infrastructure, also shape the virtual environment and provide guidelines for online interaction. Furthermore, these architectural principles have shaped a new ecology for free speech online. Most importantly though — as will be argued next — these principles seem to be a central point of reference for the lawmaker seeking to regulate free speech online.

The main thesis underpinning this paper is that the architectural choices supporting Internet design should be addressed holistically as to the significance they bear for legal enforcement: rather than addressing the Internet architecture as an online ruling deity competing with the rule of law, it is suggested that we focus on the synergy between Internet architecture and law. Returning to the focal point for this paper, free speech, the main objective of the paper is to demonstrate how decentralised Internet architecture can provide a means for promoting free speech and thus a sustainable platform for online communications. As a result, decentralisation is more than a simple design choice; it provides an ideal environment for free expression to flourish online and as such maintaining an open and decentralised net architecture should be considered as both a means and an end to online free speech. To understand this better, the next section scrutinises both architectural assumptions which form the basis for the Internet’s design: modularity and End-to-End. In what follows next, each principle is described and subsequently assessed on the merit of its capacity to promote free speech.

3. Free speech values and Internet architectures

3.1. Modularity and free speech

The Internet’s fundamental mechanism built along the lines of a layered model demystifies and unravels the source of its internal balance: a hierarchy of layers that are interlinked yet separate from one another. This unique architecture is attributed to the design principle of modularity (Baldwin and Kim, 2000). Stemming from early economic theories on decomposability of complex systems, the principle of modularity entails a system’s division to its components, the “modules.” Modules are “quasi autonomous subsystems that can be designed separately” (Aoki and Ando, 2002) while they can still work together [14].

To this cause, the designer distinguishes two types of information, visible and hidden. Namely, some information is visible to all modules in a system and defines the parameters of each module’s interaction with the others, while some information remains hidden, *i.e.*, it refers to internal matters of each module and its access is restricted to the module’s interface. The visible information constitutes the system’s design rules and is not allowed to undergo any change. On the contrary, the module designer is free to experiment and apply alterations to the hidden information within each module on the condition that it will abide by the general design rules. This easy implementation of design changes at various points within a complex system grants the system plasticity. This plasticity in turn reduces the system’s inflexibility and promotes creativity. Regarding personal computers for instance, peripheral devices connected externally (for example printers) or internally (for example, a modem) to a computer, can develop their design independently of the computer’s design, as long as they adhere to the general interface standards [15].

Layered architecture consists of modules assigned to a number of layers and creates a vertical hierarchy among them. This means that each layer contains information about its internal rules that is unavailable to other layers. Moreover, each layer can only use the services of lower layers. Therefore, the layered version of modularity that is adopted as an architectural design for TCP/IP creates a vertical hierarchy of progressively elaborated layers of specialised services. As a result, the complexity of the system is reduced, as layers operate in abstraction, without having overall knowledge of the way other layers’ functions. Moreover, the possibilities of technical flaws are diminished as the implementation occurs gradually at each level after it has been tested [16].

It can be argued that effectively all layers work by design on a purely operational level; namely, they can neither control the flow of information in general nor discriminate the routing of certain types of information. To them, all that matters is to perform the tasks they were assigned and pass on the data to the next level. Their actions cannot transcend their layer's boundaries and the raw data included in the encapsulated packets they receive is of no special importance to them. As a result, not only is it easier to publish information online, but also the message becomes independent from its medium, simultaneously allowing broader accessibility and device independence (Berners-Lee and Fischetti, 1999).

The detailed description above highlights the architectural significance of modularity in terms of ascribing specific values to handling the information flow. Although a mere engineering principle that has limited value to legal considerations regarding free speech, modularity appears to be offering great protection from censorship. Data online is routed by transparent layers, each responsible for carrying out a procedural task without the ability to discriminate information. Constructed in a layered vertical hierarchy, Internet infrastructure is marked by the integrity of its layers. Each performs a separate task and does not interfere with other layers. By employing the design of modularity on a layered infrastructure, the Internet becomes a truly neutral decentralised communications platform built on open architectural standards of separate transparent layers that route information regardless of its content.

This feature of modularity seems to reflect the principle of content neutrality in the United States' First Amendment (Stone, 1983). By applying strict scrutiny on content-based restrictions of speech, the First Amendment has sought to establish that the marketplace of ideas cannot be manipulated to put certain messages across. As the U.S. Supreme Court has noted in *Mosley*: "above all else, the First Amendment means that Government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." [17] Modularity seems to have the same effect, at least in principle, which applies to both state and non-state mandated restrictions. Equality of speech regardless of its content, which is at the heart of the First Amendment (Karst, 1975), is now also possible online; the engineering principle of modularity seems to be encoding the legal doctrine of content neutrality online [18].

3.2. The End-to-End principle and free speech

The layered model of TCP/IP Protocol is an architectural design based on normative engineering principles, the most important of which is the "End-to-End" principle. Solum and Chung (2004) describe the End-to-End as "a guiding normative principle that clarifies, articulates and illuminates the implicit design principle inherent to layers model of the TCP/IP." Initially presented as a design principle by MIT researchers Saltzer, Reed and Clark (1984), it "may be viewed as part of a set of rational principles for organizing such layered systems." The End-to-End principle suggests the following basic design: keeping the network simple while placing its intelligence at its ends. Namely, the network should only be endowed with the task of efficiently transmitting datagrams; "everything else should be done at the fringes" (Carpenter, 1996). In short, the principle can be summarised in the dichotomy "stupid networks" [19] and "smart applications". Initially, the question that was examined in the paper introducing the End-to-End principle was where the application level functions should be built; in the centre of the network (low level implementation) or at its ends, the application level (higher level implementation)? The answer, according to Saltzer, Reed and Clark (1984), was that "the function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communications system" [20]. One example is the function of the file transfer application that ensures the delivery of uncorrupted data. Although the check for any errors in data delivery could be performed at the lower level of the network communication system, it is better to place this function at the higher level of application as the lower layer may lack all the necessary information to fully perform the required function. On the contrary, the application level has the knowledge and ability to check for corrupted files, just before these reach the user and not while they are still being routed in the network (Solum and Chung, 2004). In this way, the possibility of data being corrupted is minimised and its integrity is guaranteed.

This initial thought quickly evolved into a broad architectural statement about what belongs to the network level (including the network, transport and application levels) and what should be edge-oriented; left completely to the user himself to install, configure, upgrade and maintain (Blumenthal and Clark, 2001). The adopted approach was that applications should follow the End-to-End principle so as to survive partial network failures.

As a result, End-to-End makes the network flexible and enables it to work with all sorts of data, or as Lessig eloquently puts it, "End-to-End codes a kind of neutrality" (Lessig, 2000) to the network. In this way, the Internet maintains a flexibility in its design as all users can contribute to its architecture. Platform configuration depends on the user's ability to create and implement additional software; control over its architecture "becomes separable from network ownership", granting end users the "non-discriminatory ability to design the architecture of a communication platform" aside from those who own and control its infrastructure (Bar and Sandvig, 2000). Consequently, competitiveness is increased, as neutrality towards data nurtures creativity and experimentation.

In the absence of a hierarchical entity that could discriminate against certain types of applications while favouring others, innovators were given the opportunity to directly test the appeal their applications have to users [21]. Moreover, the cost for innovation has dropped significantly as there is no need to configure settings in all layers for its implementation, but simply to invest in the application layer. Innovators can therefore demonstrate their work easily and consumers can try new applications at a marginal cost or for free without depending on their network administrator for permission (Solum and Chung, 2004). According to the MIT research group that formalised the End-to-End principle, it was this specific architectural design that enabled experimentation and led to protocols supporting the WWW or even the flexibility in the wide interconnection of millions of ISPs online (Chen and Jackson, 1998). It is because of End-to-End that innovation online became a decentralised commons, administered at a low cost by anyone that had an internet connection. This architectural design realises the main ambitions and goals of the researchers that created the Internet: the common sharing of resources on an open interlinked platform. Moreover, it shapes online culture as well; a culture of users that freely build, share, transform and develop all sorts of information regardless of its content online.

Above all, the End-to-End principle encodes online one of the main U.S. First Amendment concepts: “active listening” (Grimmelmann, 2014). This term describes the communicative process envisioned in the First Amendment as a bilateral dialogue: the speaker has the autonomy to disseminate information and the listener retains the freedom of avoiding unwanted speech that violates his integrity. Online, the listener is not passive but is actively seeking information with the added ability to filter or block unwanted speech: this is possible primarily due to the End-to-End principle. Intermediaries can certainly cut in the way of this direct interactive communication online; that said, it is a design choice that enables the Internet to facilitate this interactive dialogue respecting the choices and autonomy of both sides.

4. Law encoded: Autonomy as an embedded value

The Internet’s layered structure, built on the principles of modularity and End-to-End, accounts for its general open design. In the words of Mitch Kapor, co-founder of the Electronic Frontier Foundation: “It is an open network of networks, not a single unitary network, but an ensemble of interconnected systems which operate on the basis of multiple implementations of accepted, non-proprietary protocols, standards and interfaces” [22]. In this respect, the architectural principles running through the Internet’s design provide a remarkable mechanism that implements and promotes the free speech values enshrined in the constitution. Put simply, Lessig’s axiom that “code is law” can further translate to “law encoded” since Internet architecture appears to embrace certain First Amendment doctrines.

Taking this last point a step further, maintaining distributed architectures should be perceived not only as a useful means of preserving the Internet’s sustainability, but also as a constitutional imperative for the policy-maker. It has been suggested time and again that the current legal framework protecting free speech is not fully functional online; many have gone as far as to ask for an online bill of rights. Yet, what has changed is not the right to free speech, nor its legal underpinnings, but the circumstances. The rapid centralisation of the net architecture and the high concentration levels of intermediaries have made it impossible for the state to guarantee constitutional protection for the right to free speech online. Moreover, the focus altogether has shifted from architectures promoting free speech to architectures restricting it. Unfortunately, online policy-making sees only one part of this picture; it describes a negative aspect of the right to free speech inasmuch as it protects expression from state mandated restrictions. It has been observed that content blocking and filtering can serve many purposes, ranging from national security to online safety and social or moral reasoning. In most cases, the right to free speech is restricted when it is found to be clashing with other rights, most notably privacy and intellectual property.

At the same time, there seems to be a growing demand for a positive right to online free speech, which does not oppose but complements online privacy and intellectual property. This is reflected in the latest reports by Frank La Rue, the United Nations Special Rapporteur on Freedom of Expression and Opinion: In his landmark report on technologies of surveillance [23], La Rue refers to privacy and free speech online as being interlinked and explicitly mentions the state’s obligation to promote these rights and to hold the private sector accountable for any infringements. This echoes his own 2011 report, where he further adds that the state’s duty to respect human rights is complemented by corporate responsibility born by commercial entities online [24].

Legal theorists have long debated over whether the right to free speech should be interpreted in a pragmatic manner [25], beyond the strict confinements of the traditional “hand-off” approach that only precludes state interference. Unlike other fundamental human rights, free speech maintains a very wide scope of any expressive means of communication able to convey a certain message. As a result, not only is it challenging to define the protective scope of this right in order to understand its procedural values, but free speech further presents us with an oxymoron: its conceptual elements include substantive aspects of this right, such as censorship [26]. As such, to accurately define the contours of free speech, one must readily accept that all constraints imposed on communication are in fact a precondition of expression; censorship is therefore indicative of types of speech meriting protection, ascribing a categorical value to speech [27]. In this vein, free speech principles are premised on the acceptance of the wider concept of liberty [28]: the ability to freely communicate is thus commensurate with our understanding of liberty, regardless of whether speech is seen from a consequentialist or merely ideological point of view. It therefore becomes clear that free speech is not to be merely asserted by identifying acts violating this right (*hands-off approach*); on the contrary, expression can be as free as we allow it to be: the *positive capacity to act upon one’s free will* is determined by the presence of measures that nurture liberty rather than the absence of restrictions to it [29].

Having established the significance of a positivist/pragmatic approach for the right to free speech, one can further see its value for online communications. Serving as a communicatory platform that can reach a wide audience and has a lower participatory threshold than traditional media outlets, the Internet holds a key role as an enabler of free speech. As such, it is a means of communication, whose control yields great power in terms of exerting one’s influence at a global scale. As Castells (2011) notes

> “ideas are processed in society according to how they are represented in the realm of communication. And ultimately these ideas reach the constituencies of each network depending on the constituencies’ level of exposure to the processes of communication. Thus, the control of (or the influence on) the networks of communication, and the ability to create an effective process of communication and persuasion along the lines that favor the projects of the would-be programmers are the key assets in the ability to program each network. In other words, the process of communication in society, as well as the organizations and networks that enact this process of communication, are the key fields where programming projects are formed and where constituencies are built for these projects. They are the fields of power in the network society.”

The Internet’s quality as an enabler of free speech is also well illustrated in a number of recent Internet related cases that have been of major public concern and have mobilised civil society on a global scale: WikiLeaks revelations, NSA/PRISM spying scandal and mass protests against SOPA and PIPA, although seemingly regarding rights other than free speech, such as privacy and intellectual property, all highlight the need for a positive right of free speech online and demonstrate the importance of controlling the online informational flow. The need for a pragmatic approach that strives to promote free speech online has not gone unnoticed by the policy-maker, especially given the existence of many corporations acting as info-mediaries. Advocacy groups have highlighted the need for a more proactive constitutional protection regarding free speech online. Take for example the recent Facebook decision to take down the iconic image of a naked young girl running away in tears after a Napalm bombing in Vietnam. The post, originally shared online by a Norwegian author, was deemed inappropriate by Facebook due to nudity, which clashed with their community standards and was thus removed. Article 19’s (2016) response focused on three main suggestions: (i) limited third party intermediary liability, following the Manila Principles, (ii) Respect for international free speech standards in the Terms and Conditions of online giant corporations, like Facebook, and (iii) Clarity and transparency in how decisions to take down content are being met. Such suggested measures, however, focus more on the imposed restrictions on data flow and less on enabling the user to express freely online. As such, they address the issue of online free speech through intermediation, accepting a *prima facie* centralised architecture online that is in need of regulation. However, this approach seeks free speech protection through proxies, resulting in a regulatory system that can easily succumb to paternalism by proxy, which is in charge of providing for the "public interest". Moreover, the absence of due process and the opacity that characterises automated decisions to take down online content pose serious concerns as to the legitimacy of intermediaries controlling speech online. Not only is this reflected on the erosion of public trust online, but it further creates an environment where free speech is dependent on the restrictive mechanisms created by the level of liability borne by the intermediary. However, this is far from what is put forth in this paper, namely a pragmatic approach that focuses on the positive concept of free speech online, harnessing Internet design principles of E2E and modularity. It is suggested here that a nuanced techno-legal approach should be developed that focuses more on the Internet's architecture and less on its status of "online market" managed by a handful of commercial entities.

5. Towards a free speech policy model based on decentralised Internet architecture

As noted earlier in this paper, the issue of eroded trust online seems to be the main challenge for constructing an online policy model. The general distrust towards the state following the Snowden revelations reflects well the general scepticism about the efficacy of the legal mechanism protecting free speech when applied online. On the other hand, the user equally distrusts private actors acting as online intermediaries due to their unaccountability. The rule of law seems to be in a non-dialectic relationship with the rules of the market. Could a public law policy model for free speech, based on decentralised architecture, reconcile these two fields?

This is certainly not the first time the literature discusses how code and law can shape online activity and influence each other. Reidenberg has been among the first to discuss "Lex Informatica", namely how the network technology, could be used as a tool to "effectively formulate information policy rules" [30]. Lessig, on the other hand, has been more pessimistic in finding that the code has replaced law online [31], while Shapiro (1999) has noted the quest between state and non-state actors to gain control over the code. This paper has suggested that the truth does not entirely rest with any of these propositions. While all of them make some important valid points and have greatly influenced Internet policy-making and online governance, they all seem to adopt a technologically deterministic view. It is argued here that that the net infrastructure — although it can be controlled to shape online activity — has also the capacity to promote the values protected in law. In other words, the set of architectural values embedded in a chosen design, upon which the Internet has been built, can serve an instrumental purpose inasmuch they construct an environment, where values enshrined in law can flourish: free speech is a great example in this respect.

Building on previous work by Niva Elkin-Koren and Barbara van Schewick, who have both noted the importance of the Internet infrastructure for online economic discourse, this paper suggests a similar argument for online free speech: a dialectic relationship between technology and free speech jurisprudence. Instead of examining technology as an exogenous ruling modality, it is suggested that technology ought to be perceived as an endogenous force, which can drive policy-making models that apply online. Elkin-Koren and Salzberger offer an excellent account of how technology should become endogenous to the economic analysis of the Internet:

> "The introduction of new technologies has a dialectic relationship with other processes. Legal rules and market processes may directly affect the types of technologies available by explicitly prohibiting the use of certain technologies by law or by providing certain incentives to particular technologies and not others (...) Technology should, therefore, become endogenous to the analysis, and the economic discourse should be expanded to address it." [32]

Thus, the code is not understood here as an inimical ontology: the focus is not on it being a means of control, nor on the fact that as a hybrid modality it can shape online behaviour, but on how one can reinforce the other. Of course, Internet architects were not at all preoccupied with the First Amendment or the legal underpinnings of free speech and communications. Yet, at the same time, this architectural design of an open access decentralised network generating abundance "eliminates one of the key First Amendment diversity difficulties found in mass media" [33] and holds the capacity to fully promote free speech. This, however, does not mean that free speech is guaranteed online and that Internet architecture is a reliable mechanism that can outpace constitutional protection.

At the time of writing, we stand at a crossroads: On one hand, there are those administering the code pointing the finger at the state for infringing on the user's rights. On the other hand, ICANN has been criticised for lacking legitimacy in taking important decisions affecting the user's rights. In the meantime, the market and the norms act as equalising forces. In the middle there is the user, Lessig's "pathetic dot", who has lost trust in both sides and does not seem to be easily swayed by either of the two; law or the code. Yet, as noted earlier, both law and code are only tools, which if utilised properly, can promote free speech in the digital era. Most importantly, it should be understood that Lessig's "pathetic" dot is not pathetic at all (Murray, 2008, 2007): autonomy, as the underpinning value of both the free speech and the net architecture, should be at the centre of online policy-making.

In building an open decentralised network, Internet architects brought communication and the user to the forefront, unlike other media. In return, the networked have given their consent to the main architectural values as they have consented to the rule of law. Online networks can be controlled, however legitimacy is the added parameter that contributes to their effectiveness (Murray, 2011). Furthermore, law in cyberspace is based on voluntary obedience and does not operate on the basis of enforcement (Chris Reed, 2012). In this respect, one should consider how the rule of law and the "rule of the code" both exert forms of power based on users' consent: for Law, this consent is reflected in the Constitution. For Code, consent is nurtured by the architecture. In both cases, consent is implied further by the mere fact of users' participation, and their anticipation that the values underpinning both the Law and the Code shall remain intact. On the contrary, when administrative decisions affect these values, consent is withdrawn and trust online is eroded. It is therefore in identifying the common ground in these two modalities (with a focus on substance and not on their administration) that consent can be reaffirmed.

Of course architecture, as law, is a dynamic field. Both can change and evolve over time. In free speech jurisprudence, changes are introduced through courts; although the underpinning rationales remain the same, their doctrinal interpretation does not and it should not be a static matter. In the same way, computer engineering has provisions for change in the form of "designing for tussle" (Clark, *et al.*, 2005); technologists take advantage of the deliberately flexible design to experiment with different policies and architectures that contribute better to the Internet's sustainability. One such example is IPv6: an amendment to the Internet Protocol (IP) replacing the previous regime of IPv4 to tackle the problem of address exhaustion (Deering and Hinden, 1998). In this sense, to suggest that free speech should try to catch up with net architecture [34] and influence its design would be an arduous and unnecessary task.

This paper does not suggest a stubborn preservation of Internet architecture as such, speaking on strict formalistic terms. Instead, it is argued that free speech jurisprudence, insofar as it is underpinned by autonomy, should guarantee that the Internet's design keeps promoting the autonomy of its users and their ability to make informed choices themselves. For this to be sustainable, there needs to be not only a will on behalf of the Internet engineers, but also correct structural policies on behalf of the lawmaker. As Yoo (2012) notes, the technical evolution is characterised by an ambiguity as far as its outcome is concerned. This uncertainty should also be embraced by the lawmaker (Murray, 2007), who needs to liaise with the technologists and allow them the necessary space to experiment on better designing the Internet of the future.

Internet architecture has long been a field of constant struggle for control (DeNardis, 2013). Yet, online policy-making and the overall debate on online governance seem to be focusing more on the modalities seeking to influence the architecture and less on the actual values threatened from changes to the infrastructure. As a result, the Internet's architecture has changed to enable better governmental and market regulation [35]. In *Jewel v NSA*, the EFF explained to the court about unconstitutional NSA spying techniques to search great numbers of data by installing fiber-optic splitters on the Internet backbone [36]. Exploiting the architecture to control the user and to monitor his activity is gradually becoming the norm online. It is time that Lessig's (non-pathetic) dot should be at the heart of online policy-making and be recognised as an active part instead of merely a controlled subject. Its autonomy online should be guaranteed in order to make informed choices; the First Amendment can still be a valuable tool in this respect, provided that it acknowledges distributed architecture as a means of promoting the user's autonomy.

About the author

Dr. Argyro P. Karanasiou is a Senior Lecturer in IT & Media Law at the Centre for Intellectual Property Policy & Management (CIPPM), Bournemouth University and a Visiting Research Fellow at the Information & Society Project Centre (ISP), Yale Law School.
E-mail: akaranasiou [at] bournemouth [dot] ac [dot] uk

Acknowledgments

I wish to thank Francesca Musiani and Cécile Méadel for all their support and hard work put into this publication as well as the anonymous reviewers for their valuable feedback. The usual disclaimer applies.

Notes

[1] The issue of intermediary liability is discussed here only briefly with a view to give a short overview of the new ecology and challenges for free speech in the digital era. The focus of this paper is on examining the free speech jurisprudential values as applied to online architectures; as such it does not offer an analysis of intermediary liability, a matter so widely discussed in the literature that could easily be the focal point of a separate paper.

[2] "The United Nations Guiding Principles on Business and Human Rights (UNGPs) are a global standard for preventing and addressing the risk of adverse impacts on human rights linked to business activity. ... The UNGP are informally known as the 'Ruggie Principles' or the 'Ruggie Framework' due to their authorship by John Ruggie, who conceived them and led the process for their consultation and implementation."; see https://en.wikipedia.org/wiki/United_Nations_Guiding_Principles_on_Business_and_Human_Rights, accessed 10 November 2016.

[3] In the same vein, the Global Network Initiative is an effort seeking to promote Corporate Social Responsibility and create some general guidelines. That being said, this solution is far from guaranteeing full protection for free speech, especially in cases where online companies liaise with oppressive regimes to block access to online content. A fuller protection in this respect could be promised by the Global Online Freedom Act, introduced in 2013 in the U.S. Congress but not enacted. Under this Act, Internet companies, operating in "Internet restricting" countries, would be required to publish details of their policies with regard to human rights (Brown, 2013).

[4] Mostly referred to in the literature as '*Drittwirkung*' or 'horizontal effect' of the European Convention on Human Rights (Clapham, 1993). The European legislative framework for human rights is only mentioned briefly here as it falls outside the remit of this paper.

[5] Note for example the case of *Centro Europa 7 S.r.l.* and *Di Stefano v. Italy* (application no. 38433/09) ([2012] ECHR 974) where it was held that "in such a sensitive sector as the audio-visual media, in addition to its negative duty of non-interference the State has a positive obligation to put in place an appropriate legislative and administrative framework to guarantee effective pluralism." Similarly, in *Khurshid Mustafa and Tarzibachi v Sweden* (2011) 52 EHHR 24, it was found that Sweden had failed to protect the applicant's right to receive information via satellite broadcast. Other cases of horizontal positive obligations under art 10 ECHR (although not directly referring to the internet or telecommunications) are *Appleby and Others v United Kingdom* (2003) 37 EHRR 783, *Özgür Gündem v Turkey* (2011) 31 EHHR 41; *VgT Verein gegen Tierfabriken v. Switzerland* (2001) 34 EHHR 159; *Feuntes Bobo v Spain* (2001) 31 EHRR 50 (Mowbray, 2004).

[6] "The right to Internet access is considered to be inherent in the right to access information and communication protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens. It can therefore be inferred for all the general guarantees protecting freedom of expression that a right to unhindered Internet access should also be recognized." *Yildirim v Turkey*, App. no. 3111/10, para. 31 (ECHR, 18 December 2012).

[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), [2000] OJ L 178/1 (henceforth: E-Commerce Directive).

[8] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG) in der Fassung des Beschlusses des Deutschen Bundestages vom 13. Juni 1997 (BT-Drs. 13/7934 vom 11.06.1997).

[9] Loi no. 2000-719 du 1 août 2000 modifiant la loi no. 86-1067 du 30 septembre 1986 relative à la liberté de communication.

[10] The 1996 Defamation Act’s defence of “innocent dissemination” has often been evoked in cases concerning online distributors of defamatory material. *E.g.*, *Godfrey v Demon Internet Service* [2001] QB 201, *Bunt v Tilley & Ors* [2006] EWHC 407 (QB). Note however the new defense for Web site operators introduced in Defamation Act 2013 (c.26) para 5, which seems to be overbroad in regarding also moderated content hosted online.

[11] United Nations. General Assembly. Human Rights Council, 2011. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,” A/HRC/17/27 (16 May) at paragraphs 38–48.

[12] For instance, the architecture of Gothic churches being built tall and narrow symbolizes man’s attempts to reach God (Frankl, 2000).

[13] Kesan and Shah (2006) present an excellent analysis of the regulative effects of architecture. Among the examples they use, they refer to the architecture of American malls, which is intentionally simplistic as it tends to avoid the employment of any specific theme that might involve religion, class or politics.

[14] Its theoretical framework lies at the combination of “low coupling — high cohesion”, meaning that components are interconnected loosely, while their intra-elements are tightly coherent (van Schewick, 2010).

[15] Van Schewick, 2010, p. 40.

[16] Van Schewick, 2010, pp. 47–48.

[17] *Police Dp’t v Mosley*, 408 US 92, 95 (1972); https://supreme.justia.com/cases/federal/us/408/92/, accessed 10 November 2016.

[18] This is not to suggest that all content online cannot be restricted based on its content. Filtering or blocking using specific keywords can still restrict speech based on its content in a subtle indirect manner. This paper simply highlights the fact that the net architecture by design seems to agree with the First Amendment on many accounts. What matters here is the capacity net architecture has for this, not the many ways in which the Internet architecture can be used to restrict speech and facilitate different interests.

[19] The term was coined by Isenberg (1998) and has been broadly used in describing the End-to-End principle.

[20] Saltzer, *et al.*, 1984, p. 279.

[21] Lemley and Lessig, 2000, pp. 931–933.

[22] Mitch Kapor, “EFF’s (extended) guide to the Internet,” at https://w2.eff.org/Net_culture/Net_info/EFF_Net_Guide/EEGTTI_HTML/, accessed 20 October 2015.

[23] “76. States’ human rights obligations require that they not only respect and promote the rights to freedom of expression and privacy, but protect individuals from violations of human rights perpetrated by corporate actors. In addition, States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights. Human rights obligations in this regard apply when corporate actors are operating abroad.
77. States must ensure that the private sector is able to carry out its functions independently in a

manner that promotes individuals' human rights. At the same time, corporate actors cannot be allowed to participate in activities that infringe upon human rights, and States have a responsibility to hold companies accountable in this regard." A/HRC/23/40 (17 April 2013)

[24] "45. While States are the duty-bearers for human rights, private actors and business enterprises also have a responsibility to respect human rights. In this regard, the Special Rapporteur highlights the framework of 'Protect, Respect and Remedy' which has been developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. The framework rests on three pillars: (a) the duty of the State to protect against human rights abuses by third parties, including business enterprises, through appropriate policies, regulation and adjudication; (b) the corporate responsibility to respect human rights, which means that business enterprises should act with due diligence to avoid infringing the rights of others and to address adverse impacts with which they are involved; and (c) the need for greater access by victims to effective remedy, both judicial and non-judicial." — United Nations. General Assembly. Human Rights Council, 2011b.

[25] Barendt calls for a pragmatic approach to free speech, citing *Haig v Canada* (1993 2SCR 995, paras 68–77), where the Supreme Court of Canada recognized that positive measures should be adopted by the State to make the right to free speech meaningful (Barendt, 2005, p. 107).

[26] Fish, 2002, p. 200.

[27] Schauer, 1998, p. 160.

[28] Alexander and Horton, 1983, p. 1,356.

[29] Berlin, 1969, pp. 121–122.

[30] Reidenberg, 1998, p. 584.

[31] "We are no more ready for this revolution than the Soviets were ready for theirs. We, like (the Soviets), have been caught by a revolution. But we, unlike them, have something to lose." (Lessig, 1999, p. 234).

[32] Elkin-Koren and Salzberger, 2004, p. 106.

[33] Berman and Weitzner, 1995, p. 1,624.

[34] Unfortunately, the classic legal approach in law is to evaluate a new technology on the grounds of its relationship with the existing constitutional standards. In this sense — contrary to what is argued here — the lawmaker tries to match the online policies to the off-line word in a revisionist manner, trying "to understand the power of the new in the context of the old." (Price, 2001, p. 1,904).

[35] "Just as architecture is changing to better enable government regulation, so too is architecture changed to make the Net more like real space — more like real space, but threatening to regulate even more than real space. Better, more efficient regulation through code than the regulation effected in real space through code and contract." (Lessig, 2000, p. 997)

[36] "Plaintiffs Jewel, Knutzen and Walton's motion for partial summary judgment," at https://www.eff.org/document/plaintiffs-jewel-knutzen-and-waltons-motion-partial-summary-judgment.

References

Lawrence Alexander and Paul Horton, 1983. "The responsibility of a free speech principle," *Northwestern University Law Review*, volume 78, pp. 1,319–1,357.

Masahiko Aoki and Haruhiko Ando, 2002. *Mojuru-ka: Atarashii sangyo akitekucha no honshitsu = Modularity*. Tokyo: Toyo Keizai Shinposha.

Article 19, 2016. "Facebook vs Norway: Learning how to protect freedom of expression in the face of social media giants" (14 September), at https://www.article19.org/join-the-debate.php/251/view/, accessed 25 September 2016.

Carliss Y. Baldwin and Kim B. Clark, 2000. *Design rules*. Volume 1: *The power of modularity*. Cambridge, Mass.: MIT Press, pp. 63–92.

François Bar and Christian Sandvig, 2000. "Rules from truth: Communication p[olicy after convergence," *Proceedings of the 28th Telecommunications Policy Research Conference (TPRC) on Communication, Information and Internet Policy* (Alexandria, Va.).

Eric Barendt, 2005. *Freedom of speech*. Second edition. Oxford: Oxford University Press.

Isaiah Berlin, 1969. "Two concepts of liberty," In: Isaiah Berlin. *Four essays on liberty*. London: Oxford University Press.

Jerry Berman and Daniel J. Weitzner, 1995. "Abundance and user control: Renewing the democratic heart of the First Amendment in the age of interactive media," *Yale Law Journal*, volume 104, pp. 1,619–1,637.

Tim Berners-Lee and Mark Fischetti, 1999. *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*. San Francisco: HarperSanFrancisco.

Marjory Blumenthal and David Clark, 2001. "Rethinking the design of the Internet: The end-to-end arguments vs. The brave new world," In: Benjamin M. Compaine and Shane Greenstein (editors). *Communications policy in transition: The Internet and beyond*. Cambridge, Mass.: MIT Press, pp. 91–139.

Ian Brown, 2013. "The global online freedom act," *Georgetown Journal of International Affairs*, volume 14, number 1, pp. 153–160.

Brian Carpenter (editor), 1996. "Architectural principles of the Internet," at https://www.ietf.org/rfc/rfc1958.txt, accessed 12 December 2013.

Manuel Castells, 2011. "A network theory of power," *International Journal of Communication*, volume 5, pp. 773–787, and at http://ijoc.org/index.php/ijoc/article/view/1136/553, accessed 10 November 2016.

T.M. Chen and A.W. Jackson, 1998. "Commentaries on 'Active networking and end-to-end arguments'," *IEEE Network*, volume 12, number 3, pp. 66–71.
doi: http://dx.doi.org/10.1109/65.690972, accessed 10 November 2016.

Andrew Clapham, 1993. "The 'Drittwirkung' of the Convention," In: Ronald St. J Macdonald, Franz Matscher and Herbert Petzold (editors). *The European system for the protection of human rights*. Dordrecht: Nijhoff, pp. 163–206.

David D. Clark, John Wroclawski, Karen R. Sollins and Robert Braden, 2005. "Tussle in cyberspace: Defining tomorrow's Internet," *IEEE/ACM Transactions on Networking*, volume 13, number 3, pp 462–475.
doi: http://dx.doi.org/10.1109/TNET.2005.850224, accessed 10 November 2016.

Hillary Clinton, 2011 "Internet rights and wrongs: Choices & challenges in a networked world" (15 February), at http://www.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm, accessed 12 December 2013.

Hillary Clinton, 2010. "Remarks on Internet freedom" (21 January), at http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm, accessed 12 December 2013.

Julie E. Cohen, 2016. "The regulatory state in the information age," *Theoretical Inquiries in Law*, volume 17, number 2, pp. 369–414, and at http://www7.tau.ac.il/ojs/index.php/til/article/view/1425, accessed 10 November 2016.

Stephen Deering and Robert Hinden, 1998. "Internet protocol, version 6 (IPv6) specification," at http://www.ietf.org/rfc/rfc2460.txt, accessed 12 December 2015.

Laura DeNardis, 2013. "Internet points of control as global governance," *Centre for International Governance Innovation, Internet Governance Papers*, number 2, at https://www.cigionline.org/sites/default/files/no2_3.pdf, accessed 12 December 2015.

Laura Donohue, 2013. “Bulk metadata collection: Statutory and constitutional considerations,” *Harvard Journal of Law and Public Policy*, volume 37, number 3, pp. 757–900.

Lilian Edwards, 2013. “Privacy, law, code and social networking sites,” In: Ian Brown (editor). *Research handbook on governance of the Internet* Cheltenham: Edward Elgar, pp. 309–352.
doi: http://dx.doi.org/10.4337/9781849805049.00021, accessed 10 November 2016.

Niva Elkin-Koren and Eli Salzberger, 2013. *The law and economics of intellectual property in the digital age: The limits of analysis*. Abingdon, Oxon: Routledge.

Niva Elkin-Koren and Eli Salzberger, 2004. *Law, economics and cyberspace: The effects of cyberspace on the economic analysis of law*. Cheltenham: Edward Elgar.

Michel Foucault, 1977. *Discipline and punish: The birth of prison*. Translated by Alan Sheridan. New York: Pantheon Books.

Paul Frankl, 2000. *Gothic architecture*. New Haven, Conn.: Yale University Press.

James Grimmelmann, 2014. “Speech engines,” *Minnesota Law Review*, volume 98, number 3, pp. 868–952, and at http://www.minnesotalawreview.org/wp-content/uploads/2014/02/Grimmelmann_MLR.pdf, accessed 10 November 2016.

David Isenberg, 1998. “The dawn of the ‘stupid network’,“ *netWorker*, volume 2, number 1, pp. 24–31.
doi: http://dx.doi.org/10.1145/280437.280445, accessed 10 November 2016.

Kenneth Karst, 1975. “Equality as a central principle in the First Amendment,” *University of Chicago Law Review*, volume 43, number 1, pp. 20–68, and at http://chicagounbound.uchicago.edu/uclrev/vol43/iss1/31, accessed 10 November 2016.

Jay P. Kesan and Rajiv Shah, 2006. “Setting software defaults: Perspectives from law, computer science and behavioral economics,” *Notre Dame Law Review*, volume 82, number 2, pp. 583–634, and at http://scholarship.law.nd.edu/ndlr/vol82/iss2/2/, accessed 10 November 2016.

Neelie Kroes, 2013. “How we’re boosting trust in the cloud, post PRISM” (3 July), at http://ec.europa.eu/commission_2010-2014/kroes/en/blog/trust-cloud-prism, accessed 12 December 2013.

Mark Lemley and Lawrence Lessig, 2000. “The end of end-to-end: Preserving the architecture of the Internet in the broadband era,” *UCLA Law Review*, volume 48, pp. 925–988.

Lawrence Lessig, 2006. *Code*. New York: Basic Books.

Lawrence Lessig, 2000. “Symposium: Cyberspace and privacy: A new legal paradigm? Foreword,” *Stanford Law Review*, volume 52, number 5, p. 987–1,001.

Lawrence Lessig, 1999. *Code and other laws of cyberspace*. New York: Basic Books.

Viktor Mayer-Schönberger and Kenneth Cukier, 2013. *Big data: A revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.

Andrew Murray, 2011. “Nodes and gravity in virtual space,” *Legisprudence*, volume 5, number 2, pp. 195–221.
doi: http://dx.doi.org/10.5235/175214611797885684, accessed 10 November 2016.

Andrew Murray, 2008. “Symbiotic regulation,” *John Marshall Journal of Computer and Information Law*, volume 26, number 2, pp. 207–228, and at http://repository.jmls.edu/jitpl/vol26/iss2/1/, accessed 10 November 2016.

Andrew Murray, 2007. *The regulation of cyberspace: Control in the online environment*. Milton Park, Abingdon: Routledge-Cavendish.

David Post, 2009. *In search of Jefferson’s moose: Notes on the state of cyberspace*. Oxford: Oxford University Press.

Monroe Price, 2001. “The newness of new technology,” *Cardozo Law Review*, volume 22, numbers 5–6, pp. 1,885–1,913.

Chris Reed, 2012. *Making laws for cyberspace*. Oxford: Oxford University Press.

Joel Reidenberg, 1998. “Lex Informatica: The formulation of information policy rules through technology,” *Texas Law Review*, volume 76, number 3, pp. 553–593.

J.H. Saltzer, D.P. Reed and D.D. Clark, 1984. “End-to-end arguments in system design,” *ACM Transactions in Computer Systems*, volume 2, number 4, pp. 277–288.
doi: http://dx.doi.org/10.1145/357401.357402, accessed 10 November 2016.

Frederick Schauer, 1998. “The ontology of censorship,” In: Robert Post (editor). *Censorship and silencing: Practises of cultural regulation*. Los Angeles: Getty Research Institute for the History of Art and the Humanities, pp. 147–168.

Andrew Shapiro, 1999. *The control revolution: How the Internet is putting people in charge and changing the world we know*. New York: PublicAffairs.

Lawrence Solum and Minn Chung, 2004. “The layers principle: Internet architecture and the law,” *Notre Dame Law Review*, volume 79, number 3, pp. 815–948, and at http://scholarship.law.nd.edu/ndlr/vol79/iss3/1/, accessed 10 November 2016.

Geoffrey Stone, 1983. “Content regulation and the First Amendment,” *William & Mary Law Review*, volume 25, number 2, pp. 189–253, and at http://scholarship.law.wm.edu/wmlr/vol25/iss2/2, accessed 10 November 2016.

Barbara van Schewick, 2010. *Internet architecture and innovation*. Cambridge, Mass: MIT Press.

United Nations. General Assembly. Human Rights Council, 2011. “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,” A/HRC/17/27 (16 May), paragraphs 38–48, at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, accessed 10 November 2016.

Christopher S. Yoo, 2012. *The dynamic Internet: How technology, users, and businesses are transforming the network*. Washington, D.C.: AEI Press.

Editorial history

Received 6 November 2016; accepted 10 November 2016.