Our Internet and Freedom of Speech 'Hobbled by History': Introducing Plural Control Structures Needed to Redress a Decade of Linear Policy

Article · January 2012

CITATIONS
0

1 author:

Zach Bastick
Lille Catholic University
7 PUBLICATIONS **8** CITATIONS

SEE PROFILE

Our Internet and Freedom of Speech 'Hobbled by History': Introducing Plural Control Structures Needed to Redress a Decade of Linear Policy

This paper details and interprets evidence of the historical shift of internet control, and particularly the control of the Domain Name System, from a public trust to private parties. It examines the ramifications of these shifts on (i) political dynamics and user autonomy in the Internet's infrastructure, (ii) 'freedom of speech', and, more generally, (iii) the power of the Internet to influence individuals and to shape societies. It concludes that future policy should recognise the possibilities of non-linear and plural control structures as alternative mechanisms for promoting greater eInclusion, eAccessibility and democratisation than is permitted by the hierarchical control structures of Internet History. Within this context, the paper notes that Internet free speech and future priorities of global society are being seeded at this very moment by policies of Domain Name System and Internet architecture control that need to be more fully and more publicly monitored.

Zach Bastick

Information Technology and Anglophone Culture (CATI) Research Centre

Université Sorbonne Paris-IV, France

Keywords

Free Speech, Domain Name System Policy, Internet Privatisation, ICANN, Internet Governance

> "The enactment of policy that encourages technical non-linearity and is sensitive to multiple social, political and economic networks may foster a more flexible and organic outlook for an Internet that recognises participation at every level of its structure, more fully promotes eInclusion and eAccessibility, and genuinely democratises the network."

1. Introduction – A property analysis of DNS controls on information liberties

The first decade of the public Internet has been marked by a continual confrontation of property ideologies, not only as to how the Internet should be managed, but also by whom. This confrontation resulted in technical choices and jurisprudence that tended towards central control and linearity. These favoured short-term stability but, by reducing the structure of the Internet to a hierarchy of control, negated alternative possibilities of building a structure for eInclusion and eAccessibility that was plural and flexible at all levels. Policy resistance towards non-linear and distributed control can be explained by the contemporary worldviews of the socio-political and technical interests directing the development of the Internet, and by attempts to harmonise the new and potentially innovative ecosystem to existing legislation for existing technologies and existing paradigms. With the benefit of over a decade of hindsight, this paper now analyses evidence of the confrontation of ideologies which marked the development of the Internet to provide the basis for a more socially and politically sensitive framework for future Internet policy.

In this paper, detailed evidence of the ways in which the Internet developed is analysed to deduce that two conflicting interests have prevailed in its development - private property versus public trust - and that the conflicting expansion of these interests implies current ramifications on policy development. The current concern, then expressed, is whether policies should (i) define the Internet as private property - to be divided between those with means to develop it, and in line with their commercial interests - or whether they should (ii) define the Internet as a public trust - for promotion of information sharing and free expression of opinions, in short, for the promotion of informed free speech. This vital debate inevitably demands examination of the fundamental interests having directed Internet policy and selected its governance, so as to determine the nature of the Internet and the consequent shaping of our global social and political priorities for eAccessibility and eInclusion.

A purely technical analysis of the Internet might consider the technology as little more than a massive communication network: a mechanism for sharing information on an unprecedented scale. Yet the choice of what information is to be shared, which social groups will control the expression of, and access to, such information, and which interests will benefit from its use, are of considerable importance to the development and sustainability of society in general. Indeed, the multitude of interests which exert influence over the Internet, be they research, social or commercial, and the diverse motivations for which each party uses the network for communication, be it from privacy or security to free speech or information control, raises often competing relationships among user interests.

The balanced consideration of competing interests for future policy is perhaps best encompassed in the partly theoretical study of what is termed here as 'Internet freedom' - that is, the freedom of information afforded on the Internet. It is hence of substantial importance to consider to what extent freedom may exist on the Internet and, in doing so, to analyse the very processes which allow for its existence. To such an end, this paper analyses the Domain Name System (DNS) as the foundational mechanism allowing for Internet freedom and, further, applies property ideology in order to offer an innovative and comprehensive understanding of the evolution of Internet freedom. To this end, the privatisation of the Domain Name System is analysed through a discussion of the introduction of private sector parties in the process of Internet governance, the effects of such privatisation on information liberties, and attempts at impeding privatisation. It is through such a retrospective understanding that the current state of Internet freedom, as exclusively afforded through the DNS, can perhaps most clearly be understood, and a framework for future policy development that is sensitive to complex, non-linear socio-political interests can most explicitly be distilled.

2. Retracing the Early Privatisation of the Domain Name System

Being originally a research-oriented network, the structure of the Internet has been largely modelled on the public interest, rather than the private. The original packet-switching network, the ARPAnet, was established by the Department of Defense's Advanced Research Project Agency (DARPA) which, having standardised the network in October 1967, and continued funding its development throughout the next decade, managed the network until the early 1980s. The maintenance of the network comprised of two major aspects, which directly granted access and the dissemination of information. First, the publication and organisation of a series of non-binding documents, titled 'Request For Comments' (RFC), sought public consideration in standardising technical parameters and procedures of the network for the purpose of furthering development (Denardis, 2009: 26). Secondly, the assignment of IP addresses and the regular updating of a crucial list of Internet numeric identifiers and names were required for the operation and continued growth of the Internet (Feinler, 2011: 74-75). These functions collectively became known as the Internet Assigned Numbers Authority (IANA) (National Telecommunications and Information Administration, 2011).

For 28 years from 1969, the management of the numeric identifier and names list was delegated to Dr. Jon Postel, originally a graduate student at the University of California in Los Angeles (UCLA), who would eventually relocate his functions to the Information Sciences Institute (ISI) at the University of Southern California (Denardis, 2009: 26). There being no formal contract to explicitly state the authority of Postel in relation to other Internet responsibilities, his IANA duties were based largely, if not entirely, on the consensus of the then-small and homogeneous Internet technical community (Feld, 2003: 340). As a memorial RFC acknowledged, Dr.Postel would "keep track of all the protocols, the identifiers, networks and addresses and ultimately the names of all the things in the networked universe" (RFC2468, 1998: 1). As the network grew in size and efforts needed to maintain the list of names and numbers became greater, Dr.Postel delegated, under the discretionary authority vested in IANA, part of the duties of IANA to the Stanford Research Institute (SRI) (see RFC1174, 1990). However, the maintenance of the list soon became an impracticable and inflexible task (RFC799, 1981, p. 1), and IANA began to develop the Domain Name System (DNS) to help improve this function. Starting in the early 1990s, the new DNS would be shifted from an administrative task to become a lucrative commercial business in its own right.

The involvement of the private sector in the Internet was perhaps first seen in a secondary network that was funded by the National Science Foundation (NSF), NSFNET. NSF provided funding for the development of the network to a coalition of two commercial companies, IBM and MCI, with the Merit Network of Michigan's public universities. The size of the network increased tremendously during the beginning of the 1990s; indeed, performance statistics collected and maintained by the Merit Network indicate that the number of hosts on the network almost doubled from 617 000 hosts in October 1991, to 1 136 000 in October 1992 (Merit, 1997), and that bandwidth usage more than doubled from 1 879 bytes in October 1991, to 3 903 bytes in October 1992 (Merit, 1995). The rapid growth of the network prompted NSF to solicit proposals to manage directory services and manage registration services, including domain name registrations, for the non-military portion of the network (NSF9224, 1992). Furthermore, being an agency of the United States Government, NSF proposed an estimated $ 2 million in annual federal 'funding' for the project (NSF9224, 1992). In 1993, NSF announced that AT&T and General Atomics had been respectively chosen to provide directory services and information services, and that Network Solutions Inc. (NSI) was chosen to provide registration services for the network (National Science Foundation & Network Solutions, Incorporated, 1993). Hence, NSI, through its cooperative agreement with NSF, became the first commercial company to maintain massive control over registration services for non-military Internet domain names. NSI maintained authority over the DNS until the expiry of the agreement on September

30th 1998, after which the Department of Commerce granted authority to the Internet Corporation for Assigned Names and Numbers (ICANN), which has since continuously maintained this authority (Department of Commerce, 1998b).

The selection of NSI to manage the entirety of registration services for the network placed the private company at the forefront of the procedure for public expression on the Internet. In all practical terms, domain name registration is one of the first steps towards using the Internet as a means of expression. In order to locate an information-sharing host on the Internet, a unique numeric identifier, called an 'Internet Protocol' (IP) address, is attributed to each networked host. An IP address is implemented as a string of four sets of numbers, separated by periods, such as '192.168.0.1'. The domain name registration agreement allowed NSI to manage the creation of records which, in turn, allow for relatively obscure IP addresses to be resolved to more memorable alphanumeric 'domain names' (RFC1480, 1993). Domain names follow a hierarchical structure that is useful in roughly organising hosts on the network into general categories. Specifically, this allowed for an organisation of the network into seven generic top-level domains (gTLDs), which were available to the general Internet public, as well as over two hundred country-code top-level domains (ccTLDs) which were made available and organised at the discretion of individual countries. NSI would maintain direct control over mapping domain names to IP addresses, and it would hold responsibility for registering these maps daily on the root servers of the Internet. Hence, even though the Internet was largely a public network and, as Lessig notes, "…was born at universities in the United States" (Lessig, 1999, p. 25), it would be directly regulated by a single private company.

3. The Extent of 'Speech' on the Domain Name System

Prior to considering any evaluation of the practical ramifications of DNS privatisation on the freedoms of the network, and particularly on free speech, it is important to first qualify the extent to which domain names constitute expression that may be protected under the laws and ideals of free speech. The issue has arisen in legal actions against NSI, where two principal judicial stances have been assumed on the issue, most notably by two separate court rulings, the first being countered by the second. At the turn of the millennium, the law had been only tepidly applied to the Internet: as the Second CircuitCourt has stated, albeit within the context of trademark law, attempting to apply law "…in the fast-developing world of the Internet is somewhat like trying to board a moving bus" (*Bensuran v. Restaurant King, 1997*) and, within another case, the Court later stated itself to be "wary of making legal pronouncements based on highly fluid circumstances, which almost certainly will give way to tomorrow's new realities"(*Name Space, Inc. vs. Network Solutions, Inc., 2000*). Nevertheless, the arguments which are at first presented, and those that are then assumed in these rulings, are of foundational importance to the practical operation of Internet governance - the direct ramification of explicit judicial decisions is to form the legal framework which has manipulated the private sector actors of Internet governance in their policies regarding freedom of speech on the Internet.

Although it may be an established presupposition beyond the legal institution that "the right to express oneself in the creation of an Internet name is guaranteed by the First Amendment to the US Constitution and the People's Communication Charter, and is highly encouraged"(Name.Space, n/d), the legal stance towards the issue is less straightforward. The extent to which free speech may be protected or infringed through the DNS has been discussed in a series of court hearings during the late 1990s, almost all of which were the initiatives of legal action taken against NSI. The first of the series began after PgMedia, the alternative domain provider which would later become Name.Space, alleged First Amendment violations against NSI and the NSF (*pgMedia, Inc. v. Network*

Solutions, Inc., 1999). The court decided against the allegations, stating that domain names are not expressive speech, and cannot therefore be protected under free speech. In its argumentation, the court simplified domain names to 'source identifiers' akin to telephone mnemonics, such as 1-800-FLOWERS[1], which themselves are not considered to express speech. It was also stated that a 3-character gTLD was not substantial enough to be speech. The plaintiff appealed to the Court of Appeals in *pgMedia, Inc. v. Network Solutions, Inc.* (1999), which revised the previous ruling so as to recognise the potential expressive value of a domain, although stating that domain names in their current form do not constitute freedom of speech. It should perhaps be noted that a similar ruling was reinstated in a 2000 lawsuit, which also drew a resemblance to telephone and social security numbers, and stated that "domain names were not designed, intended, or traditionally employed to act as a fora for speech" (National A-1 Advertising, inc. v. Network Solutions, 2000).

The court rulings show a significant misunderstanding of the DNS. As was acknowledged in *Name. Space, inc. v. Network Solutions* (2000), existing 3-character gTLDs are only non-substantive "afterthoughts" due to non-technical limitations set on the DNS. Indeed, as the Court of Appeals continued, "the district court did not address the possibility that longer and more contentful gTLDs like '.jones for president' and '.smith for senate' may constitute protected speech, such as political speech or parody" (Name.Space, inc. v. Network Solutions). Yet even with the assumption of such a possibility, both courts seem to ignore that a domain name in its entirety may consist of expressive speech. In this sense, a domain name as a whole - that is, consisting of both a top-level-domain and of a second-level-domain[2] - may be expressive. For instance, the domain JonesForPresident.com is clearly expressive and may be protected under free speech, even though the gTLD itself is not. Further, this paper herein proposes that domain names may be of significant importance to the issue of free speech in that they are accessories to free speech, at least to the extent that they act as portals to protected speech.

Indeed, the uniqueness of domain names coupled with the choice of their registration process imposes a censorship requirement which implies that free speech is handed out on a 'first com[e], first serve' basis. In effect, if JonesForPresident.com has already been registered, no new user can decide to acquire the domain in order to ease the sharing of their speech – which is not so much expressed through the content of the domain itself, but through the website to which the domain points. Instead, users are forced to choose less popular extensions, such as .net or .org[3], which might themselves be of uncertain availability, in order to express themselves. The discrepancy in gTLD popularity as a factor in free speech is not substantially considered in the *Name.Spaceand pgMedia* rulings, nor is it viewed as an impediment to free speech by the judiciary in general. Indeed, a further suit initiated against NSI rather superficially concludes that "impeding access to a domain name is not the same thing as impeding access to the Internet… a web site's content is not connected to or restricted by the domain name under which it is accessed" *(Lockheed Martin Corp. v. Network Solutions, Inc., 1999)*.

The proposal of this paper, then, is that whether or not a domain name can be expressive in itself, although important in a more limited scope and although clearly possible, gives way to a larger issue of eAccessibility; considering that domain names are unique, and their distribution limited, it can be

1 The 2nd Circuit Court of Appeals notes that the adoption of the telephone mnemonic analogy to domain names is not new, citing the Ninth Circuit decision in Panavision Int'l, L.P. v. Toeppen (1998); seeName.Space Inc. v. Network Solutions Inc.(2000).

2 In a hierarchical view, a second-level-domain is the part of a domain name below the top-level-domain, and is identified as the part of the domain name which proceeds the final period in a domain name (RFC 920, 1984). For instance, in EFF.org, EFF is the second-level-domain.

3 Popularity differences among gTLD usage can be shown in registration statistics. As of May 2011, there were 973 million .com registrations, as opposed to only 14 million .net registrations and 9 million .org registrations (Internet Corporation for Assigned Names and Numbers, 2011)

seen that the current domain system imposes stringent and unnatural requirements on free speech. Likewise, although free speech on the Internet may resemble the publication of books in a library, it is the control of the keys to the library which also determine the freedom of speech. Indeed, the right to free speech is most certainly important and may be afforded, although to an uncertain extent, through the DNS, but the visibility of free speech is just as crucial in affording free speech - for free speech is of little effect when the expressive element is present but access is lacking.

4. The Effects of Early Domain Name System Privatisation on Free Speech

The early privatisation of the DNS, and particularly its monopolisation by NSI, provided a large degree of inflexibility within the growth of the Internet. Whereas IANA had previously rested largely upon community participation in developing and maintaining the DNS, NSI held little obligation towards the public and became a clearing-house for deciding upon which names would be registered. Indeed, NSI had been accused of routinely refusing to register names that it considers to be objectionable, and has justified this by claiming "a right founded in the First Amendment to the U.S. Constitution to refuse to register, and thereby publish, on the Internet registry of domain names words that it deems to be appropriate" (cited in *Name.Space, Inc.v. Network Solutions, Inc. and National Science Foundation*, 1999). Such a reference to the constitutional protection of freedom of speech may appear contradictory, as NSI seems to have applied its advantageous contractual status in order to privilege its own private interests over those of an entire infrastructure for expression. After NSI had refused to register approximately thirty domains proposed by National A-1 Advertising, Inc., under the pretence that the domains contained sexually-oriented words and phrases, National filed suit against NSI for first amendment violations (see *National A-1 Advertising, inc. v. Network Solutions*, 2000).

The court deemed that domain names were not a public forum afforded first amendment protection, and that NSI is not capable of violating first amendment rights, due to its contract with the federal government. Moreover, even beyond concerns related to speech limitation, the foundational privatisation of a public trust raised contempt in parts of the Internet community (Lioy, Maino, et al., p.1, 2000). Perhaps due to a general maturing of both camps, it would be in the latter half of 1990s that the distinct division between the application of public and private property ideologies would be perhaps most visible, specifically through the development of alternative networks that would initially bypass NSI, NSF and, ultimately, U.S. Government control of Internet-based expression.

4.1. Rise of the Alternative Internet as Extended Speech Production

Although Internet governance of the early 1990s tended towards private control of the Internet in general, and of the DNS in particular, the protocols and technology used to communicate over the network remained public. Furthermore, where institutionalised Internet governance had gained its power, such as over the administrative tasks that had previously been operated by IANA, its power was only enforced by a general consensus of its authority.

Indeed, the root servers that were maintained by NSI were only a central tenant of Internet control to the extent that the root servers were used to resolve domain names to IP addresses. Yet, just as a domain name could be resolved to its IP address using name servers controlled by NSI, the same domain names could equally be queried using an alternative root server, which could resolve them to

entirely different IP addresses. Even more significant, however, was the possibility of expanding the DNS name space to include further domain name extensions which the privately-regulated Internet denied. Such technical possibilities allowed for the application of alternative gTLDs and for the creation of potentially unrestricted new portals to information; that is, an alternative Internet.

The emergence of alternative networks, outside of the authoritarian reign of NSI, may have permitted much of the theoretical complications associated with the monopolistic private control of the Internet to be resolved. Kashpureff, who founded one such network, stated that the new, independent namespace came partly in response to the "lack of choice" in the current system (Diamond, 1998, p. 2). So as to not overlap the existing namespace, many networks replicated the domain name lists in the NSI root server and, additionally, introduced alternative extensions. Many such networks appeared, including most notably enhancedDNS (eDNS), Name.Space and Alternic. Alternic, which became operational on April 1st 1996, introduced new TLDs such as .porn for pornographic websites, .med for medical websites, and .exp for experimental uses, among others (Wilson, 2001, p. 61).

Name.Space introduced extensions such as .forpresident, .formayor and .microsoft.free.zone (*Name.Space, Inc. v. Network Solutions, Inc.*, 2000, §578). Such alternative domains extended the namespace so as to provide a larger degree of flexibility in registering domain names, and so as to curtail, as Kashpureff asserted, the "…fact that the control of domain-name space still lies with the US government" (Diamond, 1998: 2). Nevertheless, the alternative namespaces were not universally resolvable and were not accessible by most Internet users (*Name.Space, Inc. v. Network Solutions, Inc.*, 2000: §II). Since official requests to locate a host on the DNS necessarily had to pass through the configuration file and root servers at NSI in order to be resolved to an IP address (see PGMedia complaint v. NSI), the inclusion of these alternative domains on the Internet were under the direct control of NSI. Since NSI had not amended its root zone file to include the alternative gTLDs, these alternative domains were only accessible to those few users who were aware of the existence of alternative networks and technically-savvy enough to manually reconfigure their web browser to point to one of the alternative network's root zone file (Brophy, 2002: 14).

The implementation of alternative gTLDs predates any significant debate on name space extension by official actors, and this exemplifies how democratising the DNS alters the pace of developing Internet policy, the nature of decisions that justify that policy development, and political dynamics and user autonomy in the network infrastructure. At the time of writing, IANA maintains 310 top-level domains, including generic, country code, infrastructure and internationalised domain names (Internet Assigned Numbers Authority, 2011a).

However, some of these are not open to the general public and require industry affiliation – for example, .museum restricts registration to groups and institutions recognised by the International Council of Museums, and .aero requires registrants be affiliated to the aeronautics industry. Other domains registrars enforce civil registration restrictions, such as the .au domain which limits registrations to residents and entities registered in Australia (*.AU* Domain Administration, 2008).

Some registrars enforce direct government oversight over which names can or cannot be registered, a process which often has little democratic recourse. For example, AFNIC, which operates the French .fr domain, maintains a list of prohibited terms that is modifiable only by the Minister in charge of Electronic Communications (AFNIC, 2010: 17). Based on this list, AFNIC denies registration for many generic terms pertaining to political institutions (e.g. 'democratie.fr' and 'justice.fr'), country names (e.g. 'Vietnam.fr'), and regulated businesses (e.g. 'artisan.fr' and 'dentiste.fr'), among others, even though these domains may resolve to legitimate speech (AFNIC, 2011).

As opposed to the almost immediate TLD inclusion in the alternative namespaces of the 1990s, the inclusion of official TLDs by ICANN have been cautious. For instance, while Alternic introduced .porn as early as 1996, the official inclusion of a TLD for pornographic websites occurred only when ICANN introduced .xxx on March 31st 2011, although the inclusion had been officially proposed as early as 2000 and had been variously denied and reconsidered (Internet Assigned Numbers Authority, 2011b).

In practice, with the exception of the 2001 introduction of few generic domains such as .biz and .info to alleviate "concern over lack of choice" (Internet Assigned Numbers Authority, 2001: 1), as well as the 2009 introduction of internationalised domains to cater to the internet's multilingual user-base (Internet Corporation for Assigned Names and Numbers, 2009), introductions of new domains were rarely justified by principles of free speech and choice, but rather on individual proposals from sponsoring industries and formal cultural interests, such as has been the case with .aero or .museum (see Internet Assigned Numbers Authority, 2011b: 1-2). Debate over domain inclusion may drift to elements alien to protecting speech and ensuring choice through a neutral registration service. This was seen in the specific example of the recent .xxx TLD, in which debate can be generally divided along the three lines of whether the domain would encourage pornography production, whether the domain legitimises pornography, and whether the domain would be harmful to children (Mac Síthigh, 2010, 295-297).

The definition of the name space is, then, a challenge of ascertaining the popular desire of the global internet community and infrastructure needs from the top-down - as supported by formal institutions, interests and governments - rather than a democratic endeavour of internet users in recognising the free speech value of domains, both in themselves and as portals to information.

The existence and popularity of alternative networks spurred neither the official acceptance of the extended namespace, nor the inclusion of alternative top-level domains. In 2000, Name.Space stated in an accreditation application to ICANN that it had faith in the future success of its alternative domains and that it "…strongly believes that the gTLDs that it publishes and operates will be highly popular, and as proven by our own usage statistics, users will seek them out as they now do with 'legacy' domains" (Name.Space, 2000, §3.4).

Regarding Alternic, Kashpureff claims that at times "as much as three per cent of the Internet was running off our root name servers as opposed to the government's, which is very healthy, because that three per cent made a conscious choice to change" (Diamond, 1998, p. 6). In 1997, Name.Space [4] requested that NSI amend the root zone file to include the alternative gTLDs, an inclusion which would have allowed universal resolvability of the alternative extensions (*Name.Space v. Network Solutions*, 1999, §III).

The request was initially refused but was then referred to IANA and eventually to NSF, which would finally decline the request, reinforcing the decision with a directive that NSI not add any new gTLDs until NSF completes a then ongoing internal review of the United States' role in managing the DNS (National Science Foundation, 2002). After failing to receive the inclusion of its domains, Name. Space began legal action against both NSI and the NSF, alleging antitrust and First Amendment violations[5]. As PgMedia asserted in the oral court hearings against NSI and NSF, the limits of domain name registrations and the refusal to add new domain names is a clear prior restraint on free speech

4 The Name.Space network was originally represented by the company PGMedia, which would only become Name.Space following initial legal action against Network Solutions, Inc. Hence, both Name.Space and PGMedia are referred to herein to represent the Name.Space network, albeit at differing times.

5 The National Science Foundation was not initially included in the Name.Space complaint, but was only added as a non-party co-conspirator in a second complaint lodged on September 17th 1997, after the National Science Foundation denied the inclusion of the alternative gTLDs and issued a directive to Network Solutions, Inc. (Name.Space v. Network Solutions inc., 1999).

in that "…it says to the plaintiff, you must speak our words, .com, .net, .org; you can't speak .arts, .web, and you can only speak if your speech complies with the guidelines that we limit" (Southern District Court of New York, 1998, p.25).

However, Name.Space would lose both its case and a consecutive appeal following two court rulings[6]. Firstly, the court deemed NSI to be immune from antitrust due to its contractual status with a government agency and due to this status being in accord to the United States' policy of DNS management. Secondly, it was decided that domain names in their current form are not considered expressive speech and that they are, hence, not protected by the First Amendment.

4.2. Cyber Protests Bypass Monopoly over the Means to Free Speech

Whilst some in the alternative network community fought a legal battle against NSI and its external hierarchy, others floated the idea of a cyber-protest in favour of alternative namespace acceptance. In January 1998, Dr. Jon Postel himself organised a short-lived protest by redirecting the root servers away from the official structure (Mueller, 2002: 142). In June 1997, only a month after Name.Space requested NSI to merge the official and unofficial domain lookup tables, Kashpureff hacked the NSI root server through cache poisoning. The 'hacktivism' in which Kashpureff engaged allowed up to 90 % of the Internet to gain access to the Alternic gTLDS, without any reconfiguration of their browser (Brophy, 2002: 17). Hence, although only momentarily, the extended namespace became theoretically democratised, as the large majority of Internet users of all levels extended their reach away from the conventional Internet. Having attacked the technical underpinnings of the NSI private monopoly, Kashpureff completed his protest by then attacking the monopoly itself.

Thus, in July 1997, Kashpureff defaced the InterNIC website, which, at the time of writing, states to exist for the purpose of providing "…public information regarding Internet domain name registration services" (Internic, 2011). The defacement provided a link to the original Internic website as well as a protest stating that "by redirecting the domain name 'www.internic.net,' we are protesting the recent Internic claim to ownership of '.com,' '.org,' and '.net' which they were supposed to be running in the public interest" (*cited* in Brophy, 2002: 17).

The protest was technically successful, if only in its duration. Indeed, Kashpureff would begin the hijack on July 11, end the attack on July 14, but then become angry and start again on July 18 (Kornblum, 1997: 1). The protest was investigated by the FBI, which pushed for Kashpureff's gunpoint arrest in Toronto and his extradition to the United States in order to face wire fraud charges (Brophy, 2002, p. 18).

In retrospect, it can be seen that resistance to the privatisation of the Internet seems to have been of little impact. Whether considering the context of legal action taken by Name.Space against NSI and the NSF, the grass-root protests of Kashpureff or Postel, or even the very existence of alternative name spaces, the constant failures to take notice of a general need to reform DNS management are no less dramatic than the political history of the DNS itself.

Further, although there clearly existed a movement in opposition to NSI, and although this movement would eventually gain the support of founding Internet architects such as Postel (Feld, 2003: 342), the perspective of this movement was certainly not universal. For instance, whereas alternative networks are now hailed by some academics as the 'Outlaw Net' which defy authoritative rule and increase competition (*see* Brophy, 2002), others have labelled them as 'rogue servers' which destabilise the Internet (*see* Davidowicz, 1999: 10).

6 See Name.Space v. Network Solution (2000); and PGMedia v. Network Solutions (1999).

This latter, and rather apocalyptic scenario, implies that a public and non-monopolistic Internet would not be able to sustain an organisation capable of respecting domain name uniqueness – a view held despite there being already established solutions to this complication[7]. Nevertheless, this view is adopted by a majority of technical proponents (Feld, 2003: 351), and most probably by only a minority of idealists. Hence, one often needs not look far for literature criticising a public and decentralised Internet, or within much the same spirit, negatively construing the cyber-protest of Kashpureff as being filled with "…propaganda surrounding his motives and objections" (Davidowicz, 1999: 10). Despite protests against the disadvantages of a monopoly, and particularly the potential restrictions on free speech, DNS management has historically swayed towards private regulation.

5. Conclusions: A Change in the Perception of the Nature of the Internet

The political history of the Domain Name System presented here is relevant as a basis for considering how the structure of the Internet may be used to democratise the network and support both eAccessibility and eInclusion. Whereas the structure imposed upon the Internet by the official institutions of Internet Governance is hierarchical – policy was made by Network Solutions Inc. through contract with the National Science Foundation in the 1990s and ICANN through contract with the Department of Commerce today – considering the ability to create alternative Internets suggests the possibility of a horizontal control structure. Officially integrating alternative networks would have been a timely method of realising this possibility in the 1990s, but the decline of the alternative networks, and consequent growth of internet customs and technologies based on a hierarchal structure, renders this an anachronistic solution today. Nevertheless, the more general principle remains that integrating direct public control into structure of the DNS would not only democratise the content of the network by recognising domain names as 'speech', and so facilitating direct access to online material, but it would also democratise the Internet itself simply by providing a dynamic infrastructure more dependent upon its users.Through an analysis of the politics of the DNS one may note not only the infrastructure decisions taken in a pre-Web 2.0 Internet, but also how recent intellectual developments in how the Internet is perceived – the recognition of peer - production in the "networked public sphere" (Benkler, 2006), the value of the extended content of the "long tail" (Anderson, 2006),the importance of "generative technologies" (Zittrain, 2008), the formalisation of distributed production through GNU and Creative Commons copyright licenses, to name a few – may allow us to employ new social and technical conceptions to re-open a debate on the popularisation of the Internet's structure.

As has been shown, the Internet is rooted in public development and research, for the purpose of free information sharing. In its initial sense, the Internet has often been equated to the frontier, that region of the world where all is possible. Yet, the virtual frontier seems to have developed contrary to its natural, or at least original, freedom; it is the epitome of Rousseau's statement that 'man is born free, and everywhere he is in chains'. An appropriate allusion may perhaps be made to the Enclosure Movement of 18th and 19th century England, where common land was fenced off and transformed into private property (Boyle, 2003: 33-34); the parallels between the Enclosure Movement and the Internet are expressed most notably in Hunter's use of the phrase "the digital anticommons" (Hunter, 2003). Nevertheless, the century-old problematic of enclosure property ideology, and most notably the Lockean definition of freedom that seems to complement private property ideology so well, seems as pertinent today as it has seemed in the literature of the time:

7 Domain name uniqueness can be maintained through consensus amongst networks as to which IP addresses a domain name should resolve. Such consensus is possible through an organisational grouping of namespaces. Further, such grouping has already occurred, such as in the Open Root Server Confederation (ORSC) and PacificRoot networks (Brophy, 2002, p. 8).

The law locks up the man or woman
Who steals the goose from off the common
But leaves the greater villain loose
Who steals the common from off the goose.

The law demands that we atone
When we take things we do not own
But leaves the lords and ladies fine
Who take things that are yours and mine.

The poor and wretched don't escape
If they conspire the law to break;
This must be so but they endure
Those who conspire to make the law.

The law locks up the man or woman
Who steals the goose from off the common
And geese will still a common lack
Till they go and steal it back

(Anonymous, in Boyle, 2003, p. 33)

The privatisation of the Internet reflects more than a policy change: it reflects a change in the perception of the nature of the Internet itself. Internet Protocol addresses permit communication and sharing of information through a wide range of protocols, some of which operate in a distributed manner without third parties; but the Domain Name System and, most notably, its registration service, facilitate more immediate recognisability of services, individuals and institutions on the network. It is what allows for the creation of domains, here considered as portals to information, and hence, it is what allows non-technical users to access and browse information through the Web. The political development of the Domain Name System has provided a large literature exploring the responsibility of maintaining this means of production, from the earliest Request for Comments of Jon Postel to the White House (1997a; 1997b), Department of Commerce(1998a; 1998b) and ICANN reports, as well as academic analysis - Michael Froomkin (2011), an eminent academic expert on ICANN, in particular, clearly details the risks of a single entity overseeing the Domain Name System as being associated with political power and with economic power exerted over registrars, registries and registrants, although he finds that control over the DNS entails little geo-strategic risk. This essay has shown that by shifting such means into private and even monopolistic control, the public benefits of the Internet in communication, such as freedom of speech and autonomy over the infrastructure allowing that

speech, are minimised in relation to private interest, the extent to which these interests permit public or government advisory, and top-down decision structures. Although indirect, it is important to note, as has this paper, that this change is in effect a limiting and most fundamental mechanism of information control. In applying property ideology to the Internet, it can be seen that just as controlling information within a society in general, and even more so in an 'information society', acts as an "essential part of the process of social control" (Schiavetta&Komaitis, 2003: 1), so too does controlling the dissemination of information within society. Thus, to the extent that domain names act as portals to information, the privatisation of the Domain Name System does just that, by placing the public ability to share information under private control. Analysing the history of Domain Name System development brings to light the technical and legislative possibilities of plural and multi-dimensional control structures that no longer reduce the Internet to a hierarchal structure – one thus would no longer democratise 'from the ground up', but 'from the inside out', that is, across levels of user control. The enactment of policy that encourages technical non-linearity and is sensitive to multiple social, political and economic networks may foster a more flexible and organic outlook for an Internet that recognizes participation at every level of its structure, more fully promotes eInclusion and eAccessibility, and genuinely democratises the network.

Acknowledgments

To Liliane Gallet-Blanchard, Professor Emeritus at the Université Sorbonne Paris IV, for her review of an early version of this paper and for her support.

6. References

.AU Domain Administration (2008). Domain Name Eligibility and Allocation Policy Rules for the Open 2LDs (Policy Number 2008-05), retrieved October 1, 2011 from http://www.auda.org.au/policies/auda-2008-05.

AFNIC (2010). Naming Policy for .FR: Registration rules for .FR domain names, retrieved October 2, 2011 from http://www.afnic.fr/data/chartes/charter-fr-2010-03-16.pdf.

AFNIC (2011). Terms Subject to Prior Review, retrieved October 2, 2011 from http://www.afnic.fr/en/ressources/reference/charters/terms-subject-to-prior-review.

Anderson, C. (2006). The Long Tail: How Endless Choice is Creating Unlimited Demand, London: Random House.

Bensuran v. Restaurant King, 126 F 3d 25 (2d Cir 1997).

Benkler, Y. (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom, New Haven: Yale University Press.

Boyle, J. (2003). The second enclosure movement and the construction of the public domain. Law and Contemporary Problems, 66, 33-74.

Brophy, E. (2002). The outlaw 'Net': Opposition to ICANN's new Internet order. ACM SIGCAS Computers and Society, 32(4).

Davidowicz, D. (1999). Domain Name System (DNS) Security, retrieved August 7, 2010, from http://compsec101.antibozo.net/papers/dnssec/index.html.

Denardis, L. (2009). Protocol Politics: The Globalization of Internet Governance, Cambridge: The MIT Press.

Department of Commerce (1998a). Management of Internet Names and Addresses. Docket Number: 980212036-8146-02.

Department of Commerce (1998b). Memorandum of Understanding between the US Department of Commerce and ICANN. Washington, D.C.

Diamond, D. (1998). Whose Internet is it, anyway? Wired, 6.04. http://www.wired.com/wired/archive/6.04/kashpureff.html

Feinler, E. (2011). Host Tables, Top-Level Domain Names, and the Origin of Dot Com. IEEE Annals of the History of Computing, 33.3, 74-79.

Feld, Harold (2003). Structured to fail: ICANN and the "Privitization" experiment. In Thierer, A. & Crews C. (Eds.) Who Rules the Net?, Washington, D.C.: CATO Institute, 333-376.

Froomkin, M. (2011). Almost Free: An Analysis of ICANN's 'Affirmation of Commitments'. Journal of Telecommunications and High Technology Law, Vol. 9.

Hunter, D. (2003). Cyberspace as Place and the Tragedy of the Digital Anticommons. California Law Review, 91 (2), 439-519.

Internet Assigned Numbers Authority (2001). IANA Report on Establishment of the .biz and .info Top-Level Domains, retrieved October 2, 2011 from http://www.iana.org/reports.

Internet Assigned Numbers Authority (2011a). Report on the Delegation of the .XXX Top-Level Domain, retrieved October 1, 2011 from http://www.iana.org/reports.

Internet Assigned Numbers Authority (2011b). Root Zone Database, retrieved September 30, 2011 from http://www.iana.org/domains/root/db.

Internet Corporation for Assigned Names and Numbers (2009). IDN ccTLD Fast Track Process Launch, retrieved September 26, 2011 from http://www.icann.org/en/announcements/announcement-16nov09-en.htm.

Internet Corporation for Assigned Names and Numbers (2011). Registration Numbers per gTLD: Total Registrations as of May 2011. Access 01/10/2011 from https://charts.icann.org/public/index-registry-monthly.html.

Internic (2011). What is InterNIC?, retrieved September 29, 2011 from http://www.icann.org/faq.

Kornblum, J. (1997). AlterNIC founder arrested. CNET News, November 3, 1997, http://news.com.com/2100-1023-204904.html.

Lessig, L. (1999). Codes and Other Laws of Cyberspace, New York: Basic Books.

Lioy, A., Maino, F, Marian, M., & Mazzocchi, D. (2000). DNS Security. Paper presented at the Terena Networking Conference, Lisbon, May 22-25, 2000.

Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949, 964 (C.D. Cal. 1997) aff'd, 194 F.3d 980 (9th Cir. 1999).

Mac Síthigh, D. (2010). More than words: the introduction of internationalised domain names and

the reform of generic top-level domains at ICANN. International Journal of Law and Information Technology, 18 (3).

Merit (1995). Growth in Traffic on the NSFNET Backbone Service as Measured in Bytes, retrieved July 25, 2008, from ftp://nic.merit.edu/nsfnet/statistics/history.bytes.

Merit (1997). Growth as Reflected in the Number of Computers and Domain Names on the Internet, retrieved July 25, 2009, from ftp://nic.merit.edu/nsfnet/statistics/history.hosts.

Mueller, M. L. (2002). Ruling the Root: Internet governance and the taming- of cyberspace. Cambridge, Massachusetts: Massachusetts Institute of Technology Press.

Name.Space (n/d). General Policy: Name.Space Charter, retrieved October 1, 2011, from http://namespace.org/policy.

Name.Space (2000). ICANN gTLD agreement between National Science Foundation and Network Solutions, Inc.

Name .Space, Inc. v. Network Solutions, Inc., 202 F.3d 573 (2d Cir.2000).

National A-1 Advertising, Inc. and Lynn Haberstroh v. Network Solutions Inc., et al. 121 F. Supp. 2d 156 (D.N.H., September 28, 2000).

National Telecommunications and Information Administration (2011). IANA Functions Purchase Order, retrieved September 28, 2011 from http://www.ntia.doc.gov/page/iana-functions-purchase-order.

National Science Foundation & Network Solutions, Incorporated (1993). NSF Cooperative Agreement. NCR-9218742 (January).

National Science Foundation (2002). National Science Foundation Strategic Plan: FY 2003 – 2008. Arlington, VA: National Science Foundation.

Network Working Group (1981). Request for Comments 799: Internet Name Domains. COMSAT Laboratories.

Network Working Group (1990). Request for Comments 1174: IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status. CNRI.

Network Working Group (1993). Request for Comments 1480: The US Domain. Marina del Ray, CA: Information Sciences Institute.

Network Working Group (1995). Request for Comments 1855: Netiquette Guidelines. INTEL Corporation.

Network Working Group (1998). Request for Comments 2468: I Remember IANA. MCI. Panavision Int'l, L.P. v. Toeppen, 141 F.3d 1316, 1324 (9th Cir. 1998).

PGMedia, Inc. v. Network Solutions, Inc., 51 F.Supp.2d 389, 408 (S.D.N.Y.1999).

Schiavetta, S., & Komaitis, K. (2003). ICANN's Role in Controlling Information on the Internet. Paper presented at the 18th BILETA Conference on Controlling Information in the Online Environment. QMW, London, April 14-15.

Southern District Court of New York (1998). PGMedia,Inc. v. Network Solutions, Inc. Hearings.

Wilson, M. I. (2001). Location, location, location: the geography of the dot com problem. Environment and Planning B: Planning and Design 2001, 28, 59-71.

White House (1997a). A Framework for Global Electronic Commerce. Washington, DC: White House.

White House (1997b). Memorandum for the Heads of Executive Departments and Agencies. Washington, DC: White House.

Zittrain, J. (2008). The Future of the Internet and How to Stop it. London: Penguin Books.

Author

Zach Bastick
Information Technology and Anglophone Culture (CATI) Research Centre
Université Sorbonne Paris-IV, France
zach.bastick@gmail.com
http://www.epractice.eu/en/people/261044