Legal Rigidity and Digital Fluidity: Relationships between the State and the Internet

By Sarah Graham

| Preamble |

This paper shall focus on the transformative nature of technology, namely in facilitating criminal and terrorist activity and the unique challenges to regulation. The Internet requires a re-examination of static concepts of territorial boundaries and legal jurisdictions which contribute to uncertainty in regulation.

The Internet demands a re-examination of traditional frameworks of law and international relations, where static conceptions of territorial boundaries and legal jurisdictions are contrasted by the fluidity and affordances of the Internet. This juxtaposition of rigidity and fluidity suggests that the Internet might pose distinct challenges to legal governance systems while concurrently, legal systems and state values might be upheld and propagated through Internet regulations. Asking questions of how legal systems regulate Internet spaces uncovers a fundamental reconsideration of sovereignty and the traditional conception of the state. By interrogating these questions to identify actors in this debate and evaluating relevant legal cases, this article reveals the role of powerful state and non-state actors who disproportionately influence the values espoused and upheld by the relationship between the Internet and legal tradition. Before presenting and evaluating two case studies, the historical vision of the Internet and notions of territoriality and sovereignty are considered.

A Concise History of the Net

Although actors have sought to dissect, regulate, and assert authority over the Internet in recent decades, a brief history of the Internet reveals the formative notions of autonomy and individual liberation characterize the network. The Internet can be understood as the open and flexible network underpinned by domain naming systems, routing systems, and related technology systems owned by service providers which transmit information through TCP/IP packets to endpoints.oversimplifying the Internet process demonstrates the original visions on the internet as a “Stupid

---

1 Hunsinger, “Critical Internet Studies.”
Network,” premised on cheap, underspecified infrastructure to enable increased user control, liberating innovative energy.\textsuperscript{2} Using this definition of the Internet itself, the historical development of the Internet can be illustrated.

The development of this network is the product of historical contingency and idealistic visionaries. Through the union of United States Department of Defense projects and communities of university researchers, the cyber architecture was designed with a degree of autonomy and grounded in an idealistic notion of radically free information sharing and problem solving.\textsuperscript{3} However, as with any new frontier, the Internet presented a new landscape for regulation and governance. American cyberlibertarian John Perry Barlow’s \textit{A Declaration of Cyberspace} encapsulates the initial articulation of the debate between the cyberspace’s independence and imposed governance. The declaration disavows notions of consent of the governed, asserting to governments of the industrial world that their hostile, colonizing legal concepts of property, expression, and movement have no application in cyberspace.\textsuperscript{4} Barlow’s manifesto which rejects Internet governance in response to the US Federal Communications Commission and the Communications Decency Act (CDA) of 1996 provokes questions of independence and (inter)national influence, illustrating that although the Internet is initially both open and global, regulations and borders are subsequently applied to these spaces, as both the physical infrastructure and users exist within governed states.

**Negotiating Impressions of Digital Sovereignty**

Responses to the history and propagation of the Internet ask if the state has in fact “been killed by the Internet.” Though the influence of cyberspace has demanded reconsiderations, scholarship tends to reject such theatrical assertions, instead offering a more nuanced understanding of the Internet as influencing the specific notions of sovereignty and territoriality which are instrumentalized by powerful actors. Sovereignty, as invented in inherently Western statist terms, is defined as the externally recognized

\textsuperscript{2} Isenberg, “The Dawn of the Stupid Network.”
\textsuperscript{3} Rheingold, \textit{The Virtual Community: Homesteading the Electronic Frontier}.
\textsuperscript{4} Barlow, “A Declaration of the Independence of Cyberspace.”
authority over a state’s affairs. Within this, international legal sovereignty refers to mutual recognition of domestic legal authority.\(^5\) In contrast to Barlow’s declaration that governments “have no sovereignty [in cyberspace],” cyberspace is situated within the existing state framework and is therefore subject to notions authority and territoriality. While Internet spaces might enable transnational platforms, the Internet and its infrastructure exists in actual physical locales.\(^6\) This material reality endures within the prevailing systems of governance which has divided the planet into mutually exclusive territories.\(^7\) Using this framework, one might therefore ask what institutions govern the Internet?

Through the historical narrative of the Internet and recent legal cases, multiple actors can be identified as contending for authority and governance in cyberspace to create a multistakeholder model. In addition to institutions such as the Electronic Frontier Foundation (EFF) who exercise expertise and specific routes for cyber progression, the Internet Corporation for Assigned Names and Numbers (ICANN) is a force for governance. ICANN, registered as a non-profit in the United States, promotes technical coordination as an epicenter of the Internet community. However, ICANN is critiqued for American influence and the favoring of corporate interests. This thus reveals a second set of actors exerting control—technology corporations such as Google, Apple, Microsoft, and Facebook who through varying methods shape the Internet and its endpoints to suit their goals. Lastly, conventional state governments have sought sovereign authority over the internet within their territory through a variety of measures. Frequently cited are China’s “Great Firewall” and Russia’s sovereign RuNet which regulates and filters content flows to effectively assert control in authoritarian contexts. Ultimately, the abovementioned sovereignty negotiates authority with these varying actors within the statist system. Legal systems therefore must contend with both state and non-state actors in cases of cyberspace, as revealed in the cases of ACLU v. Reno and LICRA v Yahoo!

The negotiation between the unrestrained freedom envisioned within the Internet with notions of governance remains the focus of this article, firstly

\(^5\) Krasner, Sovereignty: Organized Hypocrisy.
\(^6\) Chaves, “The Internet as Global Platform?”
\(^7\) Mueller, Networks and States.
examined in the case of *ACLU v. Reno*. As organization formative in the legal concepts of cyberspace, the EFF engages in political participation, litigation, education, and campaigns which seeks to ensure that legal provisions protect cyberspace as a separate space free from the intrusion of territorial government. As a legal intermediary, the EFF gained support of elite political libertarians with strong ties to corporations such as Microsoft and Hewlett-Packard who tried to create legal protections between the Internet and territorial government, namely the United States. Under the First Amendment of the US Constitution, where anything online might be considered speech, the EFF perceived the CDA as inadvertently constraining important online speech through its vague definition of indecency to regulate obscenities online.  

Through a legal union between the EFF and the American Civil Liberties Union (ACLU), the case *ACLU v. Reno* resulted in a Supreme Court ruling of 7 to 2 which declared the CDA’s vague provisions which unnecessarily “chilled” protected speech as unconstitutional. Important in this case is the assignment of distinct legal status for cyberspace communications, notably premised on Western, especially American, notions of protected speech and First Amendment protection. However, amid the absence of legal restrictions or protection online, cyberspace began to be shaped by specific articulations of the law and American principles of protected speech, effectively applying a set of standards to a perceived open Internet free from any legal concepts of expression or regulation. Ultimately, this historical vision reveals instead the underlying debates and iterations of values underscore Internet conceptions of sovereignty and territoriality which are constantly negotiated alongside existing legal structures and politics.

Secondly, the case of *LICRA v Yahoo!* demonstrates a challenge to a specific “brand” or articulation of legal values set out by American law. Although a bordered Internet is seen as been antithetical to the Internet’s original idealism, traditional notions of state sovereignty prevail. LICRA, a French anti-Semitic non-profit filed a civil suit against Yahoo US and Yahoo’s French affiliate alleging that Yahoo allowed the posting of illegal Nazi and Third Reich memorabilia in violation of French code which prohibits the wear and sale insignias which recall organizations declared illegal in the Nuremberg Charter.

---

8 Wu and Goldsmith, *Who Controls the Internet? Illusions of a Borderless World.*
As the case progressed through French court in 2000, it was confirmed that Yahoo’s auction of such items through the site is prohibited, despite arguments made by Yahoo under the US First Amendment.9

Within this consideration between the sovereign state jurisdiction and the transnational nature of the Internet, this case reveals that states are capable of enforcing domestic law over foreign Internet companies operating within another state’s borders, supporting to counterclaim that the Internet has not in fact “killed” the notion of the state. This case recalls the significance of freedom of expression and protected speech debated by the CDA of 1996. As the Internet is a transformative medium of communication and speech, these cases are a selection of numerous international cyber-related cases which reveal the underlying contestation over the governance and sovereignty of speech.10 Here, each case illustrates competing notions of speech, where the American “cyberlibertarians” interpret the First Amendment as guaranteeing an absolute right to free speech while the European model adopts a framework that balances free speech with the right to be free from discrimination or harassment based on national identity or race.11 These cases illustrate the nuanced differences of Western states between values and notions of protected speech as dictated by law must be negotiated through new mediums such as the Internet.

**Conclusion**

The cases of *ACLU v. Reno* and *LICRA v. Yahoo!* broadly reveal the role of powerful state and non-state actors as political intermediaries who disproportionately influence a set of values disseminated online; in this case, the intricacies of protected speech. This relationship is further negotiated in international settings, such as conventions which have sought to regulate cybercrime within appropriate applications of sovereignty and extraterritorial investigations.12 Ultimately, American scholar Tim Wu encapsulates this argument by asserting that platforms structure who gets heard and what

---

9 “UEJF and Licra v Yahoo! Inc and Yahoo France.”
11 Daniels, “Race and Racism in Internet Studies.”
12 For analysis of ICTs and international cybercrime see: Clough, “A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization.”
“brand of law” is applied in cyberspace despite its decentralized governance structure. This illustrates which sets of underlying ideas of authority, state power, and ethics are espoused. Scholars have highlighted this system’s domination of Western, specifically American, information industries to situate themselves and the Internet as essential service platforms which shape a broad, single cyberlaw underpinned by narrow articulations of the United States First Amendment. Despite this, challenges such as LICRA v Yahoo! to this potentially pervasive and monolithic brand of cyberlaw suggests that legal systems maintain core notions of sovereignty and a bordered Internet.

Ultimately, interrogating the questions engendered by the debate between legal rigidity and digital fluidity reveals that although the Internet and quandaries of protected speech remain largely confined by state structures, the general point of reference or comparison rests within an Americanized legal tradition and technical innovation. Both government institutions and private actors who seek to advance their goals dictate this relationship. This analysis opens additional intersections for consideration such as transnational companies including Google and Facebook who are materially located in California and what implications this has on their adherence to and shaping of national and international cyberlaw.
Bibliography


