DEVELOPMENTS

Review Essay - The Middle Lane on the Information Superhighway: A Review of Jack Goldsmith's and Tim Wu's *Who Controls the Internet? Illusions of a Borderless World* (2006)

*By James Gannon**

A. A Collaborative Effort

Even before the preface, five words on the opening page of *Who Controls the Internet? Illusions of a Borderless World*[1] give us a good idea of the authors' views on the subject of Internet governance: "To our friend Larry Lessig." Indeed, many of the arguments and examples presented in the 226-page book will be familiar ground for those who have studied the work of Professor Lessig, notably his best-selling (as law-related books go) *Code and Other Laws of Cyberspace*[2] and *The Future of Ideas*[3]. The role of government, in particular that of the U.S., in shaping the architectures that underpin the Internet, the ability of government actors to use the Internet as a device of censorship and control and the potential power of open source projects to undermine this control are all central themes in *Code*. Specific examples of these and other trends, such as judicial intervention in the file-sharing movement and the ongoing state-driven censorship of the Internet in China were covered in *The Future of Ideas*. While there is much overlap between these works and *Who Controls the Internet*, the unique and distinguished backgrounds of both authors provide distinctive and often very insightful views on these familiar topics.

---

* Student Editor, German Law Journal. LL.B. candidate, Osgoode Hall Law School. Email: jamesgannon@osgoode.yorku.ca.

[1] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

[2] LAURENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (2000).

[3] LAURENCE LESSIG, THE FUTURE OF IDEAS (2001).

Jack Goldsmith, former U.S. Assistant Attorney General and current professor at Harvard Law School, belongs to the realist camp of international law scholars currently found in the U.S. In 2005's *The Limits of International Law*[4] co-written with Eric Posner he argues that international law is simply the product of states pursuing their own interest on the international stage and thus if states are unwilling to compromise or act against their domestic interests in order to further common goals, the total product of international law will never exceed the sum of the parts of each state's contributions. Therefore, argue the realists, the possibilities of what can be achieved on the international stage are limited. These, let's call them 'pragmatic', views of international law are combined with Columbia Law Professor Tim Wu's passion for network neutrality and a belief that an 'unregulated' Internet, free of interference by both state and powerful private actors, is essential to prevent centralized control over the spread of information. In the end, *Who Controls the Internet* leaves us with what still resembles a pragmatist's view of the possibility and desirability of government Internet control in balance with Lessig's confidence in the power of technology: "the story of the birth and early years of a new kind of Internet – a bordered network where territorial law, government power, and international relations matter as much as technological invention."[5]

All of these distinct yet somehow complementary viewpoints come together nicely in the introductory chapter. The book begins by examining the circumstances surrounding the French *Tribunal de grande instance* (High Court) case *LICRA c. Yahoo!*.[6] In the late 90's, a French citizen sued Yahoo for posting auctions of Nazi memorabilia on the search engine's website. Yahoo initially ignored the suit, claiming it was impossible for them to know where people are located when they visit the website. Without knowing the geographical location of each user, argued Yahoo, they would be forced to comply with every country's laws at the same time, a virtually impossible feat. This made for an interesting case study and a great example of old meets new: while Yahoo conducted all of its business online, it still had physical assets in many parts of the world including France, making it at least somewhat accountable to the laws of that country. The court eventually ruled against Yahoo, but only did so once the plaintiffs had proved that geo-identification technology had emerged over the duration of the litigation that allowed websites such as Yahoo to determine the location of their users.[7] Besides the amusing

---

[4] JACK GOLDSMITH & ERIC POSNER, THE LIMITS OF INTERNATIONAL LAW (2005).

[5] GOLDSMITH/WU, note 1, 5.

[6] *See* the U.S. appeal decision *Yahoo!, Inc. v. La Ligue Contra Le Racisme et L'Antisemitisme,* 145 F. Supp. 2d 1168 (N. D. Cal. 2001).

[7] It should be noted that Yahoo, in a rare act of good sense, removed its auctions of Nazi memorabilia from all their servers, not simply the French. For more information on the *Yahoo v. LICRA* case *see*

implication that technology advances so fast that the technological climate will have significantly evolved between the beginning and end of single trial, what this case aptly demonstrates is the central thesis of Lessig's *Code*: "Code is law." The court injunction that resulted from the LICRA case would not have been possible had the technology, or the code, had not been available to make it possible. It would appear at least in this case that technology's influence over the law is more important than the law's influence on technology. Nonetheless, the greater implication of the LICRA case, which is the main argument carried by Goldsmith and Wu throughout the book, is that as the Internet and the technologies that underlie the Web become more sophisticated and advanced, so too does governments' ability and desire for regulation and control.

B. Lessons in History

The book is divided into three sections, each containing between two and four relatively short chapters. The first section takes the reader through the birth and growth of the Internet starting with its inception in the 1960's as a collaborative project between the U.S. Department of Defence (DoD) and a small number of American universities. Over the next few decades, this extraordinary technology that allowed people from all over the world share ideas and information would quickly outgrow the government mandate that created it. The DoD predictably lost control of the world's largest computer network that was specifically designed to eschew any form of centralized control. Although key network administers such as Jon Postel and Vint Cerf remained on U.S. government payroll, they clearly had their own ideas and agendas on how this technology that the government had more or less abandoned should be regulated.

In these first chapters of the book, the authors pay a lot of attention to early "Internet scholars" such as Julian Dibell and John Perry Barlow. Although the effect of Dibell's "A Rape in Cyberspace"[8] is undeniable on how it enabled early adopters of the Internet come to terms with the full potential of the technology they were dealing with, it nevertheless appears that many prominent Internet law and digital copyright scholars – such as Wu, Lessig, Berkeley's Pamela Samuelson or free software guru Richard Stallman – overestimate the impact of these early writings.

---

http://www.lapres.net/yahweb.html for an extensive list of news reports and academic and professional articles.

[8] Julian Dibbell, *A Rape in Cyberspace, or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, THE VILLAGE VOICE, 21 December 1993, available at http://www.ludd.luth.se/mud/aber/articles/village_voice.html.

Many of those taking an academic interest in the Internet, particularly in the legal field,[9] are drawn to writings of Barlow because he puts the world of online affairs in an eloquent language that those accustomed to the offline world can understand. Nonetheless, his *Declaration of Cyberspace Independence*[10] was just that: a declaration. It seems almost paradoxical for one to "declare" that the Internet will always be ruled through chaos and anarchy, and to boldly state that no rules or laws shall ever govern it's "inhabitants". Inclusion of these works in *Who Controls the Internet* does serve the purpose of illustrating the strong optimism that surrounded the growing adoption of the Internet throughout the 90s, well characterized by the authors' assertion that "behind every vision of Internet utopianism lay the hope that connecting every human on earth might make the world a better place."[11] These musings, however, stray the reader away from the central theme and question of the book, and the reader is left hoping the authors had devoted more space to the last chapter in the first section of the book entitled "The God of the Internet."

Every PC or server directly connected to the Internet is issued a unique numerical address (such as 123.23.28.135) called an IP, or Internet Protocol, address. When a user attempts to access a website, such as google.com, the computer must first communicate with a central server that determines the IP address of the Uniform Resource Locator, or URL (http://www.google.com), entered by the user. Individuals and companies that wish to have a root dot-com or dot-net[12] address on the Web must apply to register their URL with these servers. It follows that control of these central servers, known as root authority, grants significant power over the content of the Internet.[13] In the chapter that discusses the implications of root authority, Wu and Goldsmith temporarily put aside the more policy-oriented language of the rest of the book to tell the story of Jon Postell, whom they refer to as "The God of the Internet." What makes this story so compelling is how deeply connected Postell and his "followers" felt to the growing network of computers that

---

[9] *See, for instance*, Lessig, note 2, 3 or Tim Wu, *When Code Isn't Law*, 89 Virginia Law Review, 2003, where Wu readily admits at 170 that "John Perry Barlow's prophecies, for example, have not been understated".

[10] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, available at http://homes.eff.org/~barlow/Declaration-Final.html.

[11] GOLDSMITH/WU, note 1, 27.

[12] For an example of a root dot-com address, see the new URL for the University of Virginia Law Review. The UVLR has recently moved to a root address at www.virginialawreview.org, instead of being a sub-URL of the university's website at scs.student.virginia.edu/~lawrev.

[13] *See*, MILTON L. MUELLER, RULING THE ROOT. INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE (2002), available at http://mitpress.mit.edu/catalog/item/default.asp?ttype=2&tid=8809.

they administered, and their strict adherence to a philosophy of fairness and free access. When policies enacted by the Reagan government in the 80's forced their contract for government services to undergo an open tendering process, a decade-long struggle between these network engineers and the government that hired them ensued, culminating in a week-long standoff in 1997 when Postell instructed almost all network administrators to redirect root authority to his own server.[14] Jon Postell had effectively taken the Internet hostage against what he feared was a new generation of network administrators who didn't follow the ideology of the network's original designers and instead wanted to run the URL registration as a for-profit venture. It wasn't until senior White House officials threatened serious legal consequences that the situation was finally resolved, and to this day root authority remains under U.S. government control, through an agency known as ICANN, which still has some of the original Internet architects on its board of directors.

It is a shame the authors did not contribute more to this part of the book. Not only is it a fascinating example of how a single individual held the power to incapacitate a technology that is now an integral part of the global economy, but it also begins to answer the question posed by the book's title. Postell and his followers' belief in fairness and ensuring free and open access to all users clashed with a government policy of increased control over the globe-spanning network and it is perhaps due to the more technical nature of the struggle for control over the Internet Root that led to a more cursory overview, which is disappointing considering the great implications of the events on the future of the Internet. Indeed, the culminating events of the Postell story "marked the beginning of a different age for the Internet, one in which powerful governments would begin to use threats of force to make their wills known."[15]

C. Global Effects

The second section of the book entitled "The Government Strikes Back" contrasts well with the preceding chapters. The effects of decisions made by a few key individuals and small U.S. government agencies in shaping the Internet presented in the opening chapters ripple across time and space to have massive effects on the global economy a few years later. As the ability to regulate the flow of information over the Internet became possible, so too did governments' desire to do so. The authors' main assertion here is that geography does matter, even on the Internet,

---

[14] GOLDSMITH/WU, note 1, 43.

[15] GOLDSMITH/WU, note 1, 46.

and this idea is well supported with several examples aside from the Yahoo case presented earlier.

Given the authors' background, it would have been more interesting for them to have spent less time on the "how" of government Internet regulation and more the "why." This is because the "how" of Internet regulation, the particular methods by which government control of cyberspace is achieved, is well known, and once again a subject that was covered in depth in Lessig's *Code*.[16] For these reasons, the detailed discussion of the Cisco-installed firewall that manages information flow into China[17] seems somewhat superfluous amidst the more academic-oriented discussions of why government regulation of Internet traffic is desirable and the legal means by which this can be achieved.

The idea is once again presented here that control need not be at either the user level or at the content provider level. In between the particular person accessing certain content and the person providing said content lie several intermediaries: cable lines, telephone routing stations, Internet Service Providers and even credit card companies. Thus the regulating agencies need not concern themselves with either end of the information exchange if the intermediaries, in particular large telecommunication and credit card companies, are much more conducive to government regulation.[18] This "intermediaries" theory is supported by the example of SeaLand, a former offshore oil platform that was converted into a jurisdiction-free webhosting service to provide space on the Internet for more "questionable" content.[19] However, what the operators of SeaLand soon came to understand was that without credit-card companies willing to accept payments to their customers, without telephone and satellite companies willing to carry information to local ISP's and without the ISP's willing to pass their content on the to end user, there existed several seemingly insurmountable barriers between them and their potential customers.

Goldsmith and Wu readily admit that any attempt at regulation is imperfect.[20] But like any laws that attempt to regulate or control certain behaviour, perfect

---

[16] *See*, in particular, Parts I "Regulability" and II "Regulation by Code."

[17] For a good overview of what is known as the "Great Firewall of China", *see Internet Censorship in the People's Republic of China*, available at http://en.wikipedia.org/wiki/Internet_censorship_ in_ mainland_China.

[18] *See*, in this regard, the doctoral dissertation by VAGIAS KARAVAS, DIGITALE GRUNDRECHTE: PERSPEKTIVEN DES VERFASSUNGSRECHTS IM INTERNET (*forthcoming* 2007), ms. on file with author.

[19] GOLDSMITH/WU, note 1, 65.

[20] GOLDSMITH/WU, note 1, "Challenges," 81-84.

compliance is not needed in order for the policy goals to be successful. Just as a highway speed limit won't stop people from driving faster than the locally defined speed limit, but will deter most drivers from going excessively over that limit, the filters installed by the Chinese government on every incoming and outgoing Internet communication are also imperfect in their own way. Some technically sophisticated users will install IP-masking systems to circumvent the filters, while others will simply use a code – where words like "cabbage" are understood to mean "democracy" – to avoid any of the "dangerous" words that the filter searches for. The authors' contention here is that imperfect does not mean ineffective. This view finds a comfortable middle ground between two existing viewpoints on government ability to regulate a new technology: while one camp will argue that "since the technology exists to control Internet communications, it will successfully be used to that effect" and others counter that "since other technology exists to circumvent the control measures, it will be used to that effect and control is therefore impossible," Wu and Goldsmith propose the following pragmatic and realist answer:

> "Government controls need not be perfect to be effective. The real question is whether and how circumvention of control by a few savvy users will make any difference to China's political evolution. [...] The effect of the government's control of the media, including the Internet, is not to kill all discussion of democracy, but to put any democratic movement at a major competitive disadvantage." [21]

The authors then address to the subject that has recently received the most attention from digital copyright scholars, including Wu himself: the file-sharing movement. Compared to the preceding analysis of Chinese citizens attempting to bypass government-installed filters to foster an underground democratic movement, a study of teenagers violating copyright law would seem somewhat inconsequential, but the authors approach the file-sharing phenomenon from the same analytical standpoint to draw conclusions on technology's effects on law and vice-versa. The same conclusion is reached here that was proposed in the China discussion: that after an initial period of instability, both laws and their implementation will catch-up to new technologies, and technology's effect on the political landscape is muted in the long run. One could argue that this theory seems to ignore certain realities. Even disregarding the economic effects of the Internet, which has eliminated geographic boundaries in many industries which itself has given rise to a substantial Chinese middle class and thus a great, albeit indirect, political effect, we

---

[21] GOLDSMITH/WU, note 1, 103.

have witnessed situations where the technology has had a real direct effect on political discourse.[22]

D. Back to the Future

The book ends with a lengthy discussion of how the Internet will evolve in short-term future. The last section of the book, entitled "Vices, Virtues, and the Future," still retains the "case-study" style of the previous chapters, but uses the examples presented more as archetypes of what the authors see as a continuing trend. By this point, the authors have sufficiently backed up their answer to the book's titular question (in short, the U.S. government controls the Internet, but large content providers and other national governments can still control what their respective customers and citizens will have access to) and look to more peripheral questions about government control of the Internet and what this means for the future of the technology. The authors' main contention remains something that venture capitalists and investors learned all too well in the late 1990's, the Internet does not, in fact, change everything. But it will change *some* things.

The authors begin by simply asking whether government control of the Internet, and all of the regulations and restrictions that come with it, is necessarily a bad thing. To a certain extent, it is argued that the Internet needs the government to be at all functional. Without contract law and an enforced property rights regime, there would be no (e-) commerce. Without laws against computer viruses, online fraud, spam and other such abuses, a lawless Internet would be a very dangerous, or at the very least an extremely annoying and frustrating, worldwide network.

Still, if there is to be one central theme that is carried throughout the book, it is the question of borders. When the authors speak of "Illusions of a Borderless World," the phrase acquires an added complexity after reading the book. Even if a seemingly subversive borderless technology could have an effect on to the physically bordered geographic world, any real impact of the Internet on the global political landscape has yet to manifest. Further, the idea of a borderless Internet may have been real in the nascent years of the technology, but this idea is becoming more and more of an illusion.

The word "illusions" is an interesting choice by the authors. For it is not by misconception or bewilderment that the average Internet user is lead to believe he

---

[22] Examples include information regarding the SARS outbreak in 2003 circulating among Chinese citizens despite the government's gag policy and the major role of the Internet in movements such as the Orange Revolution in Ukraine in 2004 and the Cedar Revolution in Lebanon in early 2005.

operates in an anarchic, borderless world. The virtual borders and walls have been under construction by both governments and content providers for quite some time now, but they remain invisible to most users. But like any successful illusion, the misdirection is intentional and carefully crafted, albeit in this case by many independently operating actors. Much like technologies such as television, radio and aviation, inventions that would intuitively appear to be impossible to regulate have in fact become some of the most closely-controlled and monitored mediums and industries. Like satellites, a technology that by its very nature eschews any notion of geographic borders and control, the Internet does not operate in a vacuum. It remains tightly coupled to several other intermediaries like computer hardware and telecommunication companies. The Chinese government knows that they cannot directly control human thought, but by controlling human speech and press, an effective indirect control is achieved. Similarly, regulation of intermediaries gives governments the ability to have a powerful indirect control of Internet content within their borders.

What makes *Who Controls the Internet* so compelling is not that it portrays a future where democracy and civil rights flourish in all corners of the world so long as the populace has access to the unstoppable force of the World Wide Web. Rather, its strength is that it takes a highly informed, pragmatic view of the importance of the Internet. It is against this account that the authors defend their approach to Internet control and, in particular, to their thesis that the Internet's success will depend on a type of government regulation that allows for an optimal use of the Internet. To the technology purists who believe that simply given the ability to circumvent digital controls, such controls are rendered useless, the authors provide an answer convincing in its simplicity "People will not always, or even usually, transcend technical barriers in order to connect to other people. Just as often, if not more so they will conform to the technical barriers, and the technical barriers themselves will reflect local government."[23] In furtherance of the pragmatic view, the authors do not skip to the assumption that regulation is necessarily detrimental: more localized content for users, easier conformity with local laws and standards and a restricted access to content that most users really don't want to see anyway are all benefits of these virtual, invisible borders. These arguments are reminiscent of the early writings of legal philosopher Morris Cohen. By attacking the traditional idea that property rights are invoidable, Cohen offered justification for state regulation of economic enterprise on behalf of the public good.[24] Eighty years later, the authors of *Who Controls the Internet* found that there is a place for the law and government regulation on the Internet, but too much state-control of online affairs

---

[23] GOLDSMITH/WU, note 1, 183.

[24] Morris Cohen, *Property and Sovereignty*, 13 CORNELL L. Q., 1927.

can have damaging effects on public discourse and the exchange of ideas.[25] These notions also relate to the arguments made by Professor Lessig in *Free Culture*[26] with regards to the effect of the Internet on copyright law. Lessig argues that the rising use of the Internet as a channel of media distribution will lead to more control from both government and content owners over the use and dissemination of information, and consequently culture.[27] Goldsmith and Wu acknowledge this view, but keep a balanced perspective with regard to government control of the Internet, maintaining a digital age-equivalent of Cohen's stance that government intervention in public marketplaces is required to curtail the effects of powerful private stakeholders.[28]

What the authors do make clear by the end of the book is regardless of the effects of government regulation of the Internet, such control is certainly possible. The decentralized nature of the architecture underlying the Internet will not rescue the large and ever-growing network from government control. In the end, the Internet is destined to find its place among other popular technologies such as the television and the automobile: ubiquitous and influential in its own way, but unlikely to have an impact on world events in any meaningful way by itself. Civil rights, ideas of democracy and revolutionary political movements will all start, evolve and in most cases end with people, not technology.

---

[25] Cohen's position that government control of property is required to maintain an open and competitive marketplace reflects many of the writings that Professor Wu has published with regards to net neutrality. *See for instance*, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOM. & HIGH TECH 141, 2003.

[26] LAWRENCE LESSIG: FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY (2004).

[27] *Id.*, 160: "For contrary to the rhetoric common at the birth of cyberspace that on the Internet, no one knows you're a dog, increasingly, given changing technologies deployed on the Internet, it is easy to find the dog who committed a legal wrong. The technologies of the Internet are open to snoops as well as sharers, and the snoops are increasingly good at tracking down the identity of those who violate the rules."

[28] One quote in particular from *Property and Culture* would apply quite readily to the undesirable consequences of unregulated powerful private actors on the Internet: "If there is one iota of wisdom in all the religions and philosophies which have supported the human race in the past it is that man cannot live by economic goods alone but needs vision and wisdom to determine what things are worth while and what things it would be better to do without. This profound human need of controlling and moderating our consumptive demands cannot be left to those dominant interest is to stimulate such demands," note 26, 30.