VIRGINIA JOURNAL OF LAW & TECHNOLOGY

FALL 2012 UNIVERSITY OF VIRGINIA VOL. 17, NO. 03

# The Cloud: *Boundless Digital Potential or Enclosure 3.0?*

DAVID LAMETTI[†]

[†] Former Director, Centre for Intellectual Property Policy, Associate Professor of Law, and former Associate Dean (Academic), Faculty of Law, McGill University. Thanks to music and technology guru Sandy Pearlman and the class in Analog Copyright at McGill in September 2011. I owe many of the seminal ideas in the first part of this paper to the discussion with Sandy and the rest of that extraordinary class. I would like to thank participants in the law and technology seminar at the European University Institute for very challenging comments in the early stages of this paper: Giovanni Sartor, Peter Drahos, Ben Wagner, and Benjamin Farrand. At successive stages Ben Wagner, Giorgio Resta, Roberto Caso, Maria Rosaria Marella, Matteo Ferrari, Umberto Izzo, Massimiliano Granieri, Daniel Lametti, André Lametti, Charleen Rains, Alberto Marinelli, Anupam Chander, Madhavi Sunder, André van der Walt, Hanoch Dagan, Eduardo Peñalver, Greg Alexander, Kevin Gray, Julia Powles, and Dan Grecu all provided very helpful comments. Previous drafts of this paper were presented at seminars at the Università degli studi di Trento, Roma I (La Sapienza), the Cambridge Intellectual Property and Information Law (CIPIL) seminar series, and the Fourth Progressive Property Workshop; I thank generally the participants at those meetings. My research assistants Ellen Bourque, Ian Dahlman, and Abby Shepard provided very helpful critiques and keen readings of the text.

## ABSTRACT

The Cloud presents enormous potential for users to have access to facilities such as vast data storage and infinite computing capacity. Yet the Cloud, taken from the perspective of the average user, does have a dark side. I agree with a number of writers and the concerns that they raise about privacy and personal autonomy on the Internet and the Cloud. However, I wish to voice concern over another change. From the perspective of users, the Cloud might also reduce the range of user possibilities for robust interaction with the Internet/Cloud in a manner that then prevents users from participating in the Internet as creators, collaborators, and sharers. The Cloud is "manageable" in a way the Internet was not. By focusing on the entities that provide Cloud services, I argue that we might take steps to encourage or, if necessary, force private entities to keep the Cloud open and accessible in the long term. I also posit the desirability of a publicly held Cloud to achieve this same end.

All errors remain my own. Finally, I acknowledge the Facoltà di Giurisprudenza, Università degli studi di Trento, and its LawTech Group for physical and metaphysical space, as well as the Faculty of Law, McGill University and the SSHRC for research support. Email: david.lametti@mcgill.ca.

# TABLE OF CONTENTS

I. Introduction ....................................................................192

II. The Metaphors of the Internet .......................................198
  A. A Horizontal Web ..................................................199
  B. Open Code ..............................................................200
  C. Few Control Points and Robust User Interaction .201
  D. Sharing....................................................................203

III. From the Internet to the Cloud: A New Set of Metaphors ..........................................................................207
  A. A Hierarchical, Centralized Structure ...................214
  B. Real Control Points................................................215
  C. Closed Systems (Get off My Cloud!) ....................216
  D. Streaming, Not Sharing (Service-Oriented Architecture) .........................................................217
  E. Thin Clients .............................................................218

IV. Worrisome Trends..........................................................221

V. A Continued Movement Towards Greater Control, or a Quantum Leap? ..............................................................224

VI. Avoiding Enclosure 3.0 ..................................................228

VII. Conclusion......................................................................242

## I. INTRODUCTION

The Cloud: a moniker that conjures images of fluffy white and weightless clouds in the sky appearing to float freely and boundlessly across an endless sea of celeste. But is the digital Cloud so benign? That is, does the digital Cloud float as freely as the metaphor suggests, or are there in fact fences that limit movement in the digital sky? And how strong are the digital winds that push them? And if these limits in cloud space are in fact real, do they represent other, even more serious consequences to the push for ever more digital capacity in the digital sky? Might the clouds in fact be storm clouds in the offing?

In reality, the picture coheres more with the latter, negative imagery. I propose that in fact we may be witnessing another round of "enclosure" in Cloud space that might have serious deleterious effects on what we have come to expect in the digital age: autonomy, exchange, spontaneity, and creativity, and all at a lightning pace. It has truly been the time of "the wealth of networks."[1] The advancing Cloud may also have a negative impact on the very manner in which users interact or "interface" with the net, with rapidly decreasing relative power. This change may be, in the words of Internet guru and popular author Cory Doctorow, part of a "war on general purpose computing."[2]

We owe the vocabulary of "enclosure" to Hungarian–Canadian political economist Karl Polanyi. In his seminal work, *The Great Transformation,*[3] Polanyi described the

[1] The term is borrowed from one of the best books written to date on the positive impact of the Internet, YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006). Brett Frischmann argues that we need the spillovers from sharing to realize the social benefits of IP. Brett Frischmann, *Spillovers Theory and Its Conceptual Boundaries*, 51 WM. & MARY L. REV. 801, 810 (2009). More recently, Frischmann gives a succinct account of the social value of the Internet. BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 336–45 (2012) [hereinafter FRISCHMANN, INFRASTRUCTURE].

[2] Cory Doctorow, *Lockdown: The Coming War on General-Purpose Computing*, BOING BOING (Jan. 13, 2012), http://boingboing.net/2012/01/10/lockdown.html.

[3] KARL POLANYI, THE GREAT TRANSFORMATION: THE POLITICAL AND ECONOMIC ORIGINS OF OUR TIME (1944).

enclosure movement in England in which communally integrated and collective farming practices on common lands were suppressed by authorities of the state, forcefully and sometimes brutally, in order to privatize land resources and create the conditions for a market economy in both agriculture as well as other sectors. The privatized lands became the base for market-oriented farming, while the peasant farmers displaced by the enclosures inevitably moved to the cities to become the labor force needed to fuel the Industrial Revolution. While most recent studies cite Polanyi for the enclosure of common lands, "the great transformation" itself was in Polanyi's view the commodification of human beings and their labor, necessary for the functioning of markets.

More recently, the term "enclosure" has been used by American intellectual property scholars such as James Boyle to describe the manner in which intellectual property rules and the concurrent practices of IP rights holders (for copyright, often large corporate interests) in the age of the Internet were being used to restrict access to the public domain of ideas or the information commons.[4] This is an area to which traditional copyright rules and doctrines normally afforded a reasonable degree of protection, all the while not restricting access to the works themselves or prohibiting or preventing fair uses. These newer enclosing practices included restricting access to works and impeding fair use, making use of digital locks to so restrict: Technological Protection Measures (TPMs), as well as measures found in the early rounds of digital copyright and

[4] JAMES BOYLE, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND (2008). On the conceptually related point of the public domain, see Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965 (1990); David Lange, *Recognizing the Public Domain*, 44 LAW & CONTEMP. PROBS. 147 (1981).

"copyright-plus" rules, such as the WIPO Copyright Treaties or U.S. Digital Millennium Copyright Act (DMCA).[5] This encircling and compression of the public domain was dubbed the "second enclosure movement," and the name has stuck. This practice continues today in copyright circles with increasingly stringent norms being proposed (from the WIPO Copyright Treaties, the DMCA, and the E.U. InfoSoc Directive and Copyright Directive to increasingly stringent bilateral trade treaties, the HADOPI, ACTA, SOPA, etc.). In the current environment, copyright owners are so guilty of systematic overreach that Jason Mazzone has recently coined the term "copyfraud" to describe the push by copyright holders beyond what was traditional or even what is legal.[6]

The Cloud—that is, the Internet as it evolves towards more centralized computing capacities and virtual "in the air," "over the Internet" storage—presents enormous potential for users to have access to facilities such as vast data storage and infinite computing capacity.[7] In the abstract, what could be

[5] Not traditionally part of the copyright doctrine or infringement for copying and limits to copyright, such measures included making the circumvention of a digital lock a *copyright* offense as well as creating an offense for making a work available on the Internet. As such, these measures earned the label "copyright plus" or "paracopyright."

[6] JASON MAZZONE, COPYFRAUD AND OTHER ABUSES OF INTELLECTUAL PROPERTY LAW (2011). *See also* Pierre-Emmanuel Moyse, *L'abus de droit : l'anténorme - Partie 2*, 58 MCGILL L.J. (forthcoming 2012) (employing abuse of right as a principle in the IP context); Kathryn Judge, *Rethinking Copyright Misuse,* 57 STAN. L. REV. 901 (2004) (arguing that any attempt by a copyright holder to effectively expand the purview of copyright protection to gain control over an idea or deter fair use constitutes misuse); Dan L. Burk, *Anticircumvention Misuse,* 50 UCLA L. REV. 1095 (2003) (describing the same phenomenon in the digital world).

[7] *See generally* Christopher S. Yoo, *Cloud Computing: Architectural and Policy Implications*, 36 REV. INDUS. ORGS. 405 (2011).

better for the end user? If the technology remains neutral and open, users will be given many more choices and much more power to use the ever-expanding and ever-more-potent digital means of production in ways previously impossible or even unimaginable.

Yet the Cloud, from the perspective of the average user, does have a dark side.[8] Most obviously, a number of leading writers have begun to document their hesitations mainly regarding the phenomenon of the Cloud and reduced Internet privacy and personal autonomy on the Web, as well as the impact of the Cloud on copyright issues.[9] The Cloud allows the continuation of the existing "seemingly free" Internet business model, while providing more and more access to more and more data to those mining it.[10] These concerns are real, and they certainly must give us pause. With a large quantity of personal information on the Cloud, more than social trust is needed to ensure that that information remains private and directed at the uses to which the "depositor" of the information has agreed. That Google, one of the major players on the Internet, and one of the emerging major players in the Cloud, altered recently its Internet privacy policy to allow all of its

[8] By users I mean mainly individuals, but to some extent I also mean corporate users of the Cloud as well.

[9] *See* Primavera de Filippi & Smari McCarthy, *Cloud Computing: Legal Issues in Centralized Architectures*, *in* NET NEUTRALITY AND OTHER CHALLENGES FOR THE FUTURE OF THE INTERNET 213 (Agustí Cerrillo-i-Martínez et al. eds., 2011), *available at* http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8341/7/IDP_7.pdf; Karthick Ramachandran, Thomas Margoni & Mark Perry, Clarifying Privacy in the Clouds (Feb. 4, 2011) (unpublished manuscript), *available at* http://ssrn.com/abstract=1755225; Daniel J. Gervais & Daniel J. Hyndman, *Cloud Control: Copyright, Global Memes and Privacy*, 10 J. TELECOMM. & HIGH TECH. L. 53 (2012).

[10] I thank Ben Wagner for this framing.

various component services to share user information among themselves should not surprise; but while this move is claimed to be more efficient for Google, the potential for abuse in a vertically integrated business model is all the greater.

I agree with these writers and the concerns that they raise about privacy and personal autonomy on the Internet and the Cloud. However, I wish to voice distress over another change. There is also, in my view, the distinct possibility that the Cloud could do more than simply reduce or render meaningless the concept of privacy on the Internet; from the perspective of users, the Cloud might also reduce the range of user possibilities for robust interaction with the Internet/Cloud in a manner which then prevents users from participating in the Internet as creators, collaborators, and sharers (i.e., the manner to which they have quickly become accustomed). This means that users will less and less be generating content and changing modalities of interaction through open software development and such. The Cloud is “manageable” in a way the Internet was not, and with users increasingly interacting with the Internet with relatively *less* powerful devices than computers—smartphones, tablets, and the like—this ability for Cloud service providers to control or manage users is enhanced. All of this means that users will become increasingly information takers—streamers, not sharers or downloaders—and potentially less in a position to control and influence the “direction” of the Internet.

This further round of enclosure I shall call Enclosure 3.0. Enclosure 3.0 has the potential to go beyond undermining copyright and the public domain—Enclosure 2.0—and to go beyond weakening privacy. Enclosure 3.0 has the potential to disempower Internet users and conversely empower a very small group of gatekeepers. Put bluntly, it has the potential to relegate Internet users to the status of digital sheep.

## II. THE METAPHORS OF THE INTERNET

The history of the Internet is well known. When the Internet—a network of computers and servers that was built by academics and researchers and funded by the U.S. military—was opened up to the world in the early 1990s, it did so on a series of programming assumptions and decisions that marked an interesting period of digital expansion and growth, and literally changed the world as we know it. In lay terms, the resulting architecture of the Internet was, even where implicit, fairly easy to describe in metaphorical terms. It was characterized by its horizontal nature, its lack of control points, its open code, and its ethos of sharing.

Let me address two important caveats before moving to the elaboration of these metaphors for the Internet and the Cloud. First, each set of metaphors is an ideal type that serves to describe a movement from the first to the second. I am therefore guilty of oversimplifying these categories for the purposes of describing and emphasizing this shift. Second, while I shall describe a set of metaphorical shifts from the Internet to the Cloud, there is not an either/or tipping point regarding this shift. As Cloud services become more profuse, they will continue to build and rely upon the Internet. To some extent, those original Internet platforms and access points will remain. So we will be in a fluid state as we move, as I believe we are moving, towards an increasing prevalence of users opting for Cloud-based services and a decrease in the use of some once-popular Internet services and practices. To a large extent, we are only at the beginnings of the movement towards Cloud-based services (and hence, as we shall see, there is cause to be optimistic about still being able to shape the Cloud as we would like).

As noted above, I posit that the original Internet was characterized by its horizontal nature, its lack of control points, its open code, and its ethos of sharing. I elaborate each metaphor in turn.

### A. A Horizontal Web

The Internet is a set of computers linked to servers that in turn are all linked to each other. All of these servers allow information to be broken down and to pass over the Internet in packets, with the information being finally reassembled at the end user's server. The Web was in this sense horizontal in terms of its fundamental architecture. No one route for information was necessary on the information highway.[11] There was no one check (or choke) point, as there were myriad routes over which packets could travel in order to get to their final destination for re-assembly. It is true that one needed an Internet Service Provider (ISP) in order to get "online," but by and large a wide range of ISPs—big and small, dial-up and increasingly broadband and wireless, including some free services—has meant that this is not much of an impediment.

Of course, in reality there were attempts, especially by certain governments, to create choke points and curtail the flow of information on the Internet, sometimes with success. By and large, however, the architecture has remained relatively flat, and information can often find ways around control points.

[11] *See* IXMAPS, www.ixmaps.ca (last visited Oct. 12, 2012) ("IXmaps is an interactive tool that permits internet users to see the route(s) their data packets take across North America, with 'interesting' sites highlighted along the way.").

## B. Open Code

The horizontal nature of the Internet was deliberate. The Internet was consciously conceived as an open structure. The metaphor here is interoperability: all the parts were meant to work together. As Lawrence Lessig noted in *Code*, the early programmers of Internet protocols—Tim Berners-Lee and Robert Cailliau—consciously chose to make their operating code interoperable, a practice that continues today, allowing other programmers to continue to add on.[12] When HTTP and HTML were left open by design, the Web grew exponentially thereafter, in a similar open-ended fashion.[13]

This openness is part of what has come to be called the "end-to-end" nature of the Internet's architecture.[14] From the first layer of the physical infrastructure of the Internet (i.e., the Internet's hardware), through the logical infrastructure (i.e., its TCP standards, etc., noted above), through its application layer (i.e., its programs), and then to its content and finally to a social layer (i.e., social media, networks, affiliations, and groups), the Internet was designed to preserve robustness and adaptability. In order to do so, the lowest layers of the network (i.e., physical infrastructure and then logical infrastructure) can be cast as generally as possible, while the more functional levels can be more specific.[15] In theory, the lower levels of the structure are "application-blind," meaning that they are neutral as to the more specific applications and programs that are running at higher levels. In this way, the infrastructure providers could not distinguish between users and uses. As

[12] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 103 (1999).
[13] *Id.*
[14] FRISCHMANN, INFRASTRUCTURE, *supra* note 1, at 319.
[15] *Id.* at 320 n.9.

Brett Frischmann points out, user identity was also largely obscured, given the manner in which data packets moved around using IP addresses, which were only known to the user's own ISP.[16] The "end-to-end" design, and especially the idea that end users are not distinguished by infrastructure providers, helped to sustain an "infrastructure commons" management scheme for the Internet by insulating users from market-driven restrictions on user use and access.[17]

### C. Few Control Points and Robust User Interaction

This horizontal architecture meant a decentralization of power. The Internet was comprised of many relatively powerful computers interacting. Early Internet commentators such as John Perry Barlow, cofounder of the Electronic Frontier Foundation (EFF), argued that the anarchical nature of the Internet made it a lawless zone, or no-law land, where standard IP rules did not apply.[18] For Sandy Pearlman, this horizontality is partly represented in the idea of "autonomy": users could interact freely, with little control, using powerful laptop and desktop computers. These points are linked: users using relatively powerful computing devices, and spread out around the world, results in few control points and a high degree of autonomy. That there are few control points increases

[16] *Id*. at 321.

[17] *Id*. at 322. Frischmann does point out that some blocking is possible and that the principle is under pressure currently as providers routinely begin to monitor traffic and technology develops that allows them to inspect packets. *Id*. at 322–23. But for my purposes the end-to-end principle still is the general norm and a valid Internet metaphor.

[18] John Perry Barlow, *The Economy of Ideas: A Framework for Patents and Copyrights in the Digital Age. (Everything You Know About Intellectual Property is Wrong.)*, WIRED, Mar. 1994, http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html.

the possibility for users themselves to determine how they will use the Internet.

Of course, this mythical anarchy was never going to be completely true; criminal and private law norms ranging from rules concerning child pornography to defamation and choice of law all became part of the formal normativity regulating the Internet within countries, and, through cooperation and the interaction of private international law rules and principles, across international borders.[19] Copyright and trademarks also evolved to govern formally certain aspects of behavior "online." A system of domain name governance emerged. These formal rules were supplemented by a great deal of informal normativity.[20] Furthermore, almost all broadband networks have control and choke points built in.[21] Nevertheless, the idea that there was a certain freedom in the

[19] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006), Part 2 ("Government Strikes Back"), especially chs. 4 & 5, pp 49–86.

[20] Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 VA. L. REV. 505 (2003); Mark F. Schultz, *Copynorms: Copyright Law and Social Norms*, *in* 1 PRAEGER'S INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN A DIGITAL AGE 201 (Peter Yu ed., 2006).

[21] In principle, any ISP can exhibit some control over users as ISPs are the access point to the Internet. More fundamentally, perhaps nefariously, ISPs and governments have the technology to survey content and even shape or block traffic, at least temporarily. *See* Milton L. Mueller et al., Syracuse Univ. Sch. of Info. Studies, *The Network Is Aware: Social Science Research on Deep Packet Inspection*, DEEPPACKET.INFO, http://dpi.ischool.syr.edu/Home.html (last visited May 30, 2012) (containing various studies on traffic throttling, packet inspection technology, etc.). *See also* JACK GOLDSMITH & TIM WU, *supra* note 19 at Part 2 ("Government Strikes Back"), ch. 6, ("China"), pp. 87–104 (discussing attempts by the Chinese government to block websites).

Internet space remained true. This was especially the case where formal normative responses often lagged behind technological changes: for example, by the time the provisions of the WIPO Copyright Treaties, signed in 1996, are finally enacted by all signatories, they will be—indeed are already and have long been—out of date.[22] These gaps in the formal normative response have allowed for a great many Internet practices—such as file sharing and mash-ups—to develop, evolve, and become entrenched in advance of any attempt to regulate.

### D. Sharing

This last metaphor is more controversial. In my view, the dominant ethos of the Internet, notwithstanding attempts to the contrary by major corporate copyright holders, is sharing. From the beginning, code was open. Soon thereafter content and services were shared, in movements such as wikis. Users downloaded, making their own private copies (often re-sharing down the line), or they uploaded content to be shared. Users collaborated to create, whether they produced works of art, music, literature, or wikis.[23] When attempts were made to throttle this sharing, the technology reacted with new and more effective means to share.[24] Business models began to be built on this idea.[25]

[22] In Canada, Bill C-11, incorporating some of the aspects of the treaties, passed in the summer of 2012, some sixteen years later. Copyright Modernization Act, R.S.C. 2012, c. C-42, amending the Copyright Act, R.S.C. 1985, c. C-42 (Can.).

[23] *See generally* BENKLER, *supra* note 1.

[24] This phenomenon has been noted by a number of writers. *See, e.g.*, MASSIMILIANO GRANIERI & ANDREA RENDA, INNOVATION LAW AND POLICY IN THE EUROPEAN UNION: TOWARDS HORIZON 2020 (2012). Fred

A great deal of creative activity came to be built on these sharing models. The ethic was and still is a strong one, enforced by powerful informal social norms. A leading example in this area is the development, along the same ethos as the original Internet protocols, of open source software, including popular applications like Firefox and VLC, as well as the Linux and BSD family of operating systems, developed almost exclusively by users over the Internet during the past two decades. More and more content is being made available in open access formats, using General Public and Creative Commons licenses.

In sum, the snapshot of the Internet was one with a horizontal series of exchanges and interactions, with few control points, many participants—of whom many had a great deal of computing power—with a rough equality in computing power and much shared content and capacity. Of course there were bugs in the system: private property rules, copyright rules, paracopyright rules, contractual agreements, technological incompatibility, and attempts at censorship were all employed by powerful interests to control aspects of the Internet. But the power was diffuse enough that one could always work around (if necessary "hack" around) these blockages. Usually there were enough "channels" on the Internet to make such solutions possible.

von Lohmann of the EFF has argued, using examples from various points in the history of copyright, that the lag in formal normativity meant that the technology could develop more rapidly, without impediment. Fred von Lohmann, *Fair Use as Innovation Policy*, 23 BERKELEY TECH. L.J. 829 (2008); *see also* PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: FROM GUTENBERG TO THE CELESTIAL JUKEBOX (1996).

[25] *See, e.g.*, DON TAPSCOTT & ANTHONY D. WILLIAMS, WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING (2006).

A large public domain of ideas and shared content, as well as many open source aspects of the architecture of the Internet, was created by this horizontal Internet. Yochai Benkler points out a fundamental economic and social transformation perhaps as important as the historical one identified by Polanyi: "[t]he removal of the physical constraints on effective information production had made human creativity and the economics of information itself the core structuring facts in the new networked information economy."[26] Thus the new revolution focused on ideas, creativity, and information, far from the previous importance placed on physical resources such as coal and steel and on manual human labor. Benkler goes on to underscore the importance of openness and sharing to the nature of the new revolution. He identifies the importance of non-proprietary strategies, the rise of nonmarket and production and—most radically and for my purposes most important—the rise of effective, large-scale cooperative efforts, citing peer production of information, knowledge, and culture exemplified in the open source software movements, wikis, and shared computing.[27]

As highlighted from the outset, the first attempts to enclose this digital public domain in the Internet age were through increased copyright protection and the so-called digital agenda which attempted, with varying degrees of success,[28] to expand the purview of copyright to access control through digital fences and "locks," thus reversing copyright's prior historic and conceptual focus from *copying* to including merely

[26] BENKLER, *supra* note 1, at 4.
[27] *Id.* at 4–6; FRISCHMANN, *supra* note 14, at 336–45.
[28] Certainly there was success at getting formal legislation expanding copyright beyond its usual conceptual borders. There was less success at the level of enforcement of these norms.

accessing the work, and gutting the historic balances of copyright protection (limits, fair use, fair dealing, etc.). Other provisions have expanded, somewhat illogically from a conceptual point of view, from the purview of copyright infringement to acts that might circumvent digital locks. This was labeled the "second enclosure movement" by James Boyle, sharing with Polanyi's characterization the idea that intellectual resources that were once a public good—and part of a complex normative framework—were being parceled off and privatized. As with the first enclosure movement described in *The Great Transformation*, it was a coordinated effort by those with economic and social power using political power to affect the ends of privatization.

But generally, these measures have not been all that effectual.[29] Indeed, further rounds of Internet and copyright "reform" have been proposed or enacted, most famously the "three-strikes" model,[30] precisely because earlier attempts had

[29] *See, e.g.*, Doctorow, *supra* note 2.

[30] Examples of graduated response schemes can be found in the French legislation known as HADOPI, the graduated response in Ireland scheme, as well as ACTA. *See, e.g.*, Loi 2009669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (1) [Law Promoting the Distribution and Protection of Creative Works on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jun. 12, 2009 (French creation and Internet law); Décret 2009-1773 du 29 décembre 2009 relatif à l'organisation de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet [Decree Regarding the High Authority for Transmission of Creative Works and Copyright Protection on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 29, 2009 (decree creating the High Authority for the Broadcasting of Works and the Protection of Rights on the Internet (HADOPI)); EMI Records & Ors v. Eircom Ltd, [2010] IEHC 108 (H. Ct.) (Ir.); Annemarie Bridy, *ACTA and the Specter of Graduated Response*, 26 AM. U. INT'L L. REV. 559, 576–

little impact. With regard to this latest round of measures in Enclosure 2.0, their success is equally uncertain: the jury is still out. In larger terms, the nature of the Internet has continued to remain constant in terms of the descriptive and operational metaphors described above.

## III. From the Internet to the Cloud: A New Set of Metaphors

The Cloud has the potential to alter fundamentally this open landscape, allowing for the possibility of control that might make the efforts of Enclosure 2.0 pale in comparison. By allowing for centralized online storage and processing capabilities, the Cloud is changing the metaphors that describe the Web as we have come to know it and facilitating its centralized control by a few key players.

77 (2011*)* (discussing the Irish graduated response regime)*; see also* The Anti-Counterfeiting Trade Agreement (ACTA), Oct. 1, 2011 (not yet entered into force) (*available at* http://www.ustr.gov/acta).
There is also a U.S. "six strikes regime," which was privately negotiated between ISPs and the movie and music industries in July 2011, bypassing government and courts. *See* Nate Anderson, *Major ISPs Agree to "Six Strikes" Copyright Enforcement Plan*, ARS TECHNICA (Jul. 7, 2011), http://arstechnica.com/tech-policy/2011/07/major-isps-agree-to-six-strikes-copyright-enforcement-plan/; Abigail Phillips, *The Content Industry and ISPs Announce a "Common Framework for Copyright Alerts": What Does It Mean for Users?*, ELECTRONIC FRONTIERS FOUND. (Jul. 7, 2011), https://www.eff.org/deeplinks/2011/07/content-industry-and-isps-announce-common. The enforcement and education body set up by these parties is called the Center for Copyright Information. *See* CENTER FOR COPYRIGHT INFO., http://www.copyrightinformation.org (last visited Oct. 12, 2012).

Cloud computing, in a nutshell, makes it profitable for large-scale data storage,[31] computing-capacity, and networking services[32] to move from a local general-purpose computer (a personal laptop, a desktop, or other computing device) and local server to the pooled resources of a non-local, centralized computer or computers.[33] In principle, this moves computing

[31] The National Institute of Science and Technology (NIST) provides the traditional description of the three-part structure of cloud services: *Software as a Service* (SaaS), *Platform as a Service* (PaaS), *Infrastructure as a Service* (IaaS). PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUB. 800–145, THE NIST DEFINITION OF CLOUD COMPUTING 2–3 (2011). SaaS is defined as follows: *Software as a Service* (SaaS): offers finished applications that end users can access through a thin client device such as a smartphone or tablet, usually using only a Web browser. The end user has no control over any major aspect of the design or functioning (servers, networking, and storage infrastructure) of the application. Examples of SaaS include Gmail and Google Docs. For applications of NIST's definition of SaaS, *see* YOO, *supra* note 7, at 5; Gervais & Hyndman, *supra* note 9, at 56–61; JASPER P. SLUIJS ET AL., TILBURG LAW & ECON. CTR., DISCUSSION PAPER 2011-036, CLOUD COMPUTING IN THE EU POLICY SPHERE (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909877.

[32] Computing and networking capacity are part of PaaS and IaaS, roughly defined as follows: *Platform as a Service* (PaaS): offers to the end user an operating system as well as suites of programming languages. It also offers and software development tools that customers can use to develop their own applications. Thus PaaS gives users control over application design, though not control over the physical infrastructure. Examples include Microsoft Windows Azure and Google App Engine. *Infrastructure as a Service* (IaaS): offers end users direct access to processing, storage, and other computing resources. It also allows the configuration of those resources and the capacity to run operating systems and software. Examples of IaaS include Amazon Elastic Compute Cloud (EC2) and IBM Computing on Demand.

[33] This description is known as the "outward-looking" perspective of the Cloud, following Birman, cited in YOO, *supra* note 7, at 3. According to Yoo, the "inward-looking face" worries more about how it all works: "From the inward-looking perspective of how individual cloud computing

and storage from peripherals on the "edge" of the network to the computing "core" of the Cloud.[34] So, for example, a user of traditional word-processing software such as Word or an email application such as Outlook runs these programs off her own machine, using local processing power and data storage facilities. By contrast, a Cloud-based application such as Google Docs or Microsoft Office Live for word processing or Gmail for email uses centralized, non-local capacities.

Through a process known as "virtualization," a layer of software mimics hardware and interacts with client devices (such as Google and Microsoft's servers). Client devices are effectively tricked into thinking they are dealing exclusively with the computing capacity of a single computer, when in reality they may be sharing capacity with another client device or even using more than one computer simultaneously. The model is dynamic, and tailored to the needs of the client. The result is a more efficient use of hardware and thus lowered costs, which then makes offering Cloud services, such as online storage, profitable.

There are many Clouds—private, public, or hybrid—depending in the standard lexicon on what is known as the deployment model. To clarify the argument in this Article, regarding a certain doubling of terminology, virtualization offers three ways for clients to set up or deploy their Cloud: public, private and hybrid. These categories refer to whether or not the client is interacting with dedicated hardware. The public and private Clouds that I shall discuss below, however,

elements interact with other cloud computing elements, the focus is on the ability to coordinate and integrate applications and data operating on multiple machines through mechanisms into a seamless whole." *Id.*

[34] *Id.*

refer to the public or private nature of entities providing Cloud services to users.

By way of background, let me recount briefly the traditional National Institute of Standards and Technology (NIST) categories for deployment models.[35] In terms of how Cloud services are deployed, a *private Cloud* uses combinations of all of these various deployment models through a privately controlled data center. This data center is used exclusively by the organization that has created it. Moreover, a private Cloud will commonly use proprietary technologies that are closed to other users of Cloud services. The *public Cloud*, on the other hand, is the Cloud with which the average user is the most familiar: it is Apple, Microsoft, Amazon, and Google pushing us to use their storage facilities and drop boxes for files, songs, and photos. These are corporate entities offering a wide variety of Cloud-based services to different users. That is, it is well known corporate entities—*private*, but in a different, traditional sense—that had initially provided Internet access or other Internet services that now use the excess computing capacity available to them to offer virtual storage, computing capacity, and other such Cloud services. So while this Cloud is, in a sense, open to the public—and hence *public* in the sense of "providing services accessible to the general public"—it is *privately held*. The *hybrid Cloud* contains both private, internal computing and public accessibility. In hybrid Clouds, the deployment model is usually achieved through a proprietary data center, but then the

[35] *See* MELL & GRANCE, *supra* note 31, at 3.

model employs public Cloud resources to furnish computing and storage services.[36]

The fourth deployment model—the *community Cloud*—has been thus far less discussed in the emerging literature.[37] A community Cloud is created when Cloud services are provided "for the exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations)."[38] Ownership of this Cloud may be varied: it "may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises."[39] I shall return to this model later.

By contrast, I wish to focus some attention on whether a public or private entity offers Cloud computing services (in whatever deployment model—public, private, or hybrid—is chosen). Indeed, I shall posit the possibility (and, later in the paper, the desirability in some cases) of a publicly held Cloud, which, as opposed to the current Clouds, would be built by those public and quasi-public institutions that have computing capacity and can provide Internet access. The paradigmatic example here would be universities, which already provide

[36] I thank Ellen Bourque and Anupam Chander for forcing me to be more precise on my use of "public."

[37] For example, the fourth concept is not metioned at all in Yoo, *supra* note 7, Gervais & Hyndman, *supra* note 9, or SLUIJS ET AL., *supra* note 31. *See also* Kenji E. Kushida, Jonathan Murray & John Zysman, *Diffusing the Cloud: Cloud Computing and Implications for Public Policy*, J. INDUSTRY, COMPETITION & TRADE 209, 234 (2011) (noting that "community Cloud" is "somewhat ill defined").

[38] MELL & GRANCE, *supra* note 31, at 3.

[39] *Id*.

Internet access for research, teaching, and communication for its "citizens": teachers, students, administrators. However, it could also include governments, government agencies, etc. These public or quasi-public actors might then make Cloud resources available to the general public or to community-based groups to administer.

Some skepticism has been expressed regarding the move to Cloud computing, particularly with respect to individual privacy and the use of gathered private data and information, as noted above.[40] But there is also a powerful critique founded on the impact that the process has on the autonomy of the user and her computing device. Sandy Pearlman has presented a colorful representation of this critique of the Cloud:

> In one corner, *Cloud Computing*: Designed to migrate user's applications, processes and content off local device storage and up to remote storage on the "cloud" of the Internet. Under this scenario for the next regularly scheduled Internet gold rush, hard drives become cloud drives; software becomes cloudware; music would have "no need" to reside locally on anyone's computational gadget and personal computers would have "no earthly need" to be as autonomously powerful as they've now become. After all in the vastness of this indispensable (Meta) Internet, upon which everyone would become completely dependent, all that used to be local and private will be

[40] Filippi & McCarthy, *supra* note 9, at 221; Gervais & Hyndman, *supra* note 9, at 76.

> subsumed. Autonomy – and Anonymity – would be replaced by Terminality. Just like it was in the 70s and 80s before personal computers were grown insanely powerful enough to be autonomous.[41]

The opposite, Cloud-friendly or Cloud-utopic view describes the process as moving from "siloing" of devices to more integrated models, with all the perceived potential benefits that this presents.[42] In this picture the user is empowered by the access to more computing capacity and more coordinated means of using it, and thus individual autonomy is heightened.

It goes without saying that the Cloud presents great opportunity. The resource pooling that is possible using cloud technology means lower overall costs (through lowered costs for the provider, who then offers services at lower costs to users), much more storage capacity, more effective use of excess computing capacity (and new business models based on that exploitation), resulting in a productive use of latency and better use of hardware. It also might mean better reliability over the long term.[43] Some claim that streaming music off the

[41] Sandy Pearlman, The Cloud vs. the Paradise of Infinite Storage (Or, When Infinities Collide) (Sept. 18, 2009) (unpublished manuscript) (on file with author).

[42] Richard L. Schwartz, *Why Computing Isn't Going Away, Just Hiding in the Clouds*, GIGAOM, (Sept. 10, 2011, 12:00 PM), http://gigaom.com/cloud/why-computing-isnt-going-away-just-hiding-in-the-clouds/.

[43] Though we are not here yet, businesses still tend to use the Cloud as a backup, for "mirroring" and overflow, and not yet in lieu of their own capacities. *See also* David Talbot, *Security in the Ether: Information Technology's Next Grand Challenge Will Be to Secure the Cloud—and Prove We Can Trust It*, TECH. REV., Jan.–Feb. 2010, at 40, *available at*

Cloud will save the music and film industries.[44] Yet Pearlman's skepticism, on further analysis, raises serious concerns over what one might call the dark lining of the Cloud. It is to this investigation that I now turn.

The Cloud is already becoming ubiquitous. While most users are still availing themselves to the services of the "old" Internet, many are beginning to be enticed onto the Cloud by friends inviting them to share pictures on Dropbox and such. Nevertheless, the parameters and presumptions of the Cloud are much different from the more commonly known and understood Internet whose rough lines were described above. In metaphorical terms, as compared to the Internet, the Cloud might be described as follows.

### A. A Hierarchical, Centralized Structure

The Cloud imposes a hierarchy to the Web, centralizing capacities in large computer operations with points of access at key nodes. As we become dependent on the Cloud for its central storage and computing capacity, we necessarily reveal the increasing hierarchy of the Internet and rely on it. Thus the Cloud becomes much more vertically oriented than the generally horizontally spread Internet. The Cloud will further increase the ability of cloud players to control when, where, and how users interact with the Web.

http://www.technologyreview.com/featured-story/416804/security-in-the-ether/.

[44] Farhad Manjoo, *The World's Greatest Music Service: Thank Heavens—Spotify Is Finally Available in the United States*, SLATE (Jul. 9, 2009), http://www.slate.com/articles/technology/technology/2009/07/the_worlds_greatest_music_service.html (suggesting that the availability of streaming may reduce the number of "illegal" downloads).

This move to vertical integration is part of the core business model of the Cloud. As this is a new and competitive terrain, the handful of Cloud service providers are quite naturally aggressively battling to sell "their" Cloud to users. These providers use low- or no-cost models and an integration of a wide variety of convenient services to draw users into their service model. It helps that the services, in terms of cost per unit, are extremely inexpensive to provide once the technology has been developed, thus allowing providers to maintain low costs for a long period of time in the baiting period. The hope is that consumers then get hooked. By raising the costs of switching from one provider to another, Cloud service providers further reinforce this verticality. In the long term, this increases the power of the provider vis-à-vis the user.[45]

So in short, from a horizontal base that is the Internet, users are being drawn up into one of few Clouds with the offer of easy and cheap services. But once drawn, users become increasingly dependent and hence are increasingly vulnerable to the decisions of the Cloud provider. What will happen when Dropbox is no longer free?

### B. Real Control Points

This structural hierarchy creates real control points on the Internet at the points where data is stored and computational capacity exists or is linked. These points offer places to control Internet traffic, gather data, regulate access, censor, etc., which are not as possible in a decentralized, horizontal Web. Large Internet players—Facebook, Amazon, Apple, and the like—are already those moving to marshal their

[45] I thank Dan Grecu for helping me to frame this point.

capacities on the Cloud by drawing people to their Clouds through their gateways, or what I would call their nodal points. These control points provide the very real possibility that the quantity and quality of Cloud traffic can be controlled. It is a question of gates and gatekeepers. At present, the gates to the Internet are wide open (with many points of entry and at little or no cost), but as the Cloud evolves we could see a situation where there are fewer gates and more powerful gatekeepers exercising ever greater control.

### C. Closed Systems (Get off My Cloud!)

The vertical integration model of the Cloud is based in part in providing a wide variety of integrated services, first for user convenience and, in the long term, to keep users on that system. In particular, the possibility of creating effective technological incompatibilities as a business model is further enhanced. Technological incompatibilities are the single most effective type of digital rights management strategy that exists. If the goal is to exclude, a lack of interoperability is the answer. A "closed" or "walled" garden is constructed, whose beauty is available only to the people allowed inside, who are usually those who have paid to see it. Apple has famously built its highly successful business model around incompatibility. Using a specific, requisite technology or platform, a Cloud service provider can dictate terms of engagement in a manner that was heretofore impossible on an open Internet.

Critics have already begun to call for standardized protocols,[46] but no effective means of enforcing standardization exists. In principle, it would be especially difficult to

[46] YOO, *supra* note 7, at 20; SLUIJS ET AL., *supra* note 31, at 11.

standardize the privately held Clouds, as these actors are by definition operating in the private sphere. Finally, there are problems with relying on competition law in an area of governance that changes so rapidly to help maintain a level, technologically neutral playing field. Monopolies are likely.[47]

## D. Streaming, Not Sharing (Service-Oriented Architecture)

The Cloud posits a service-oriented architecture.[48] Rather than purchase copies of what they need (and keep them forever), or download them where otherwise unavailable for purchase (and also keep forever), users purchase services on a current needs basis. It is a "pay now for what you receive now" model.[49] Obviously, this puts users at great risk if they can no longer afford the service. Users are information takers under this model, as opposed to information sharers. As they interact with the Internet with less computational capacity, users increasingly accept content and other services as opposed to generating content themselves. Open software models are potentially more difficult to maintain should Cloud providers increasingly opt for closed systems. Access to services becomes the norm, and streaming takes over from sharing as the dominant descriptive metaphor.

Daniel Gervais and Daniel Hyndman point out that many of the services currently offered on the Cloud are meant to enhance sharing. Photos, text, music, and video can all be shared on services such as Facebook and Picasa.[50] They are

[47] SLUIJS ET AL., *supra* note 31, at 17.
[48] YOO, *supra* note 7, at 3–4.
[49] I thank Dan Grecu for this phrasing.
[50] Gervais & Hyndman, *supra* note 9, at 65.

correct here: there is a whole lot of sharing going on. Two caveats are necessary, however. First, one can only share in the way the service permits and within the parameters (i.e., the software and the applications) of that system. Second, what is "shared" is ultimately controlled by the service: Facebook has claimed ownership over what is posted; while Google Drive does not formally claim ownership, its licensing request ensures that at the very least it claims de facto control over what is posted.[51] It goes without saying that the primary purpose for which any information gathered will be used is to match advertisers to a user's preferences. However, it is also true that posted material can be erased unilaterally by the service where it is against policy, such as criminal content, or is alleged to be a copyright violation, and even for matters of taste. This form of sharing is not the robust, uncontrolled, even anarchical form of sharing that we had heretofore seen on the Internet, but a limited, directed form of sharing, subject to the will (and perhaps the whim) of Cloud service providers.[52]

### E. Thin Clients

As Jonathan Zittrain continues to warn us, the nature of the devices through which we connect to the Internet and increasingly the Cloud must be kept in mind.[53] This caution

[51] *Google Drive Terms of Service Spark Privacy Concerns*, CBC NEWS, http://www.cbc.ca/news/technology/story/2012/04/25/google-drive-cloud-storage-terms.html (last updated Apr. 27, 2012).

[52] It might be argued that the move to streaming is mainly a response to the slowing down of and criminalization of file sharing. I think this is too strong a view: rather, devices make streaming easier.

[53] *See* Charles Arthur, *Walled Gardens Look Rosy for Facebook, Apple—and Would-Be Censors*, THE GUARDIAN, (Apr. 17, 2012), http://www.guardian.co.uk/technology/2012/apr/17/walled-gardens-

must be taken most seriously. We are entering a period where "thin clients" are becoming the norm. These are devices with little computing capacity or need to perform computing functions on their own. We are already beginning, overwhelmingly, to interact with the Web with these thin clients: smartphones, music players, and tablets. These perform specific, limited functions and are aimed at ease of use for the decidedly average user. Thus a smartphone or other device need not have the full capabilities of a powerful, general-purpose desktop or laptop computer. Moreover, these kinds of devices are "tethered" to their systems: the types of functions that they can perform and the applications that they run are either pre-set or controlled by the "mother" system, often remotely. One can only add other functionality to the device with difficulty, if at all; in any event, in order to get into the "walled garden" one must run the applications and software dictated by that system's "gardener." Apple, for example, has gone to great lengths to limit what iPads and iPhones can run and do, all in the name of efficiency, convenience, and security. While many users like this kind of limited but easy functionality, in doing so there is a great deal of control over hardware and software exerted by Apple. The kinds of services offered on the Cloud, coupled with the hierarchy mentioned above, open the possibility for thin clients to be effective in limiting users to only those functions deemed appropriate or necessary by the Cloud operator. The open protocols of the old

facebook-apple-censors; *see also* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2009).

Internet—HTML—are rapidly falling behind the rush to mobility.[54]

There is a marketing aspect to this "dumbing down" of devices.[55] The simplicity of the device is a powerful means of marketing (along with its styling, obviously); if it were too complicated to use, it would be less attractive. Once again, think Apple here. So while devices are still complex, they are programmed—at the outset or remotely on an ongoing basis, or both—to be simple and to not be altered by the user. Of course, there is a degree of relativity here: while no one would disagree with the proposition that a smartphone or tablet is a highly capable computing device as compared to desktops twenty years ago, the fact remains that they are simply not meant to do general purpose computing. As Zittrain points out, users cannot get easy access to the underlying software or code to write their own applications or dictate their own uses, relying on the capacities of the device.[56]

In short, it is very difficult for a user to understand how one might get these devices to do anything other than the specific tasks that they were meant to do, using the apps and services that they were meant to use (and indeed are restricted to using). Hence, they differ greatly from desktops and laptops in this regard. With a thin-client model comes the possibility of an even greater reliance on the Cloud for just about everything: content, applications, as well as the popular services (storage, computing power, etc.) that we have seen thus far. These

[54] The only exception, according to Zittrain, is the Android operating system for mobile devices that does allow for greater programmability. ZITTRAIN, *supra* note 53.

[55] I acknowledge Dan Grecu for suggesting this gloss on the "thin clients" argument.

[56] ZITTRAIN, *supra* note 53.

devices cannot be, in Zittrain's terms, "generative." Moreover, even for those so technologically capable, it is hard to envisage thin-client terminals themselves allowing easy access to IaaS and PaaS services, and maybe not even to all that many SaaS services, and certainly not in an undirected, autonomous fashion. These powerful services will be reserved to those who maintain their general computing devices.

As seen above, Pearlman has labeled this phenomenon "terminality," with its obvious "back to the future" flavor: we are moving back to interacting with the Cloud with something more akin to the dumb terminals of the past days of local area networks (even though this terminality is a product of programming and tethering, and not of the lack of potential in the hardware of the device itself). The standard user interaction with the digital world through Pearlman's "insanely powerful" laptop will be a thing of the past. Generative potential and autonomy will have been increasingly lost.

## IV. WORRISOME TRENDS

These changing metaphors are, in my view, indicative of worrisome trends at the level of architecture. The potential to control the Cloud exists in a way that was not possible for the Internet. Perhaps what we have experienced was a brief golden age: the technology of the Internet, coupled with a lack of control or formal normative attention, aligned with a traditional set of pre-digital copyright rules and the good sense to allow many truly good things to happen. It has been a period of extraordinary creativity and innovation, as fans of one Internet art form, the mash-up, and fans of open software programs will surely attest.

The lack of centralized power allowed the Internet to happen. Intellectual property rules did not get in the way. If the current trends continue, there is a real possibility that:

- The structure could be more easily controlled, more likely leading to monopolies and associated behavior (content and price control, etc.), and resulting in fewer choices for access to the Cloud than there has been for the Internet.

- Users might be baited and hooked into Cloud service reliance, and in the long term be powerless to react to unfavorable terms of use.

- Users could lose the ability to actively defend against the monopolies of computing capacity and (illegitimate) content control.

- In time, there will be less sharing in anything but the sharing that the various systems allow. Users who continue to download and share in the might get locked out *ex ante* (instead of being sued *ex post*).

- Streaming could be slowed or stopped outright where users do not pay or are deemed not to pay enough for a service.

- There would be less generative creation and innovation. Users who create derivative art forms (mash-ups and such) could get locked out, and prosecuted, and would have less possibility to create and develop collaborative works such as open source software.

- Users could lose autonomy.

In short, a user's ability to work around illegitimate blockages is circumscribed by the technology that she is compelled to use. So-called "legitimate blockages"—if you want Apple's Cloud, buy Apple's services and hardware—will be even more omnipresent and powerful. Indeed, the shift in ethos from an open-code Internet to closed Clouds will have a great impact on a user's ability to move in Cloud space.

Are these changes part of a generational shift? Are younger users less worried than the forty-, fifty-, and sixty-somethings who remember the world without the Internet and its genesis, and have gazed at it in wonder ever since? Firsthand, admittedly anecdotal, experience in the classroom and private life have tended to confirm this hypothesis,[57] but this statement is based on impressions only.

It should also be noted that the possibility of the use of encryption changes the dynamics of power relations between the actors. [58] As a tool, encryption might be used by either users or hosts to hide their content from right-holders, ISPs or other third parties. In some cases encryption may even mean that hosts do not have access to their users' data. As regards architecture, encryption would allow users to evade certain restrictions on uses, such as peer-to-peer sharing, where such exist, but here as well the parties shut out are ISPs and right-

[57] A large number of students in the Analog Copyright class did not appear to have any problem whatsoever with the move to the Cloud. There was an interesting amount of confidence, even faith, in the idea that the technology would work out any challenges. There was also a strong opinion that downloading and copying was no longer necessary in a world where one could stream just about anything anywhere.

[58] I acknowledge here the interventions of Ben Wagner and Leonardo Maccari on pushing me to think about encryption, and Ben Wagner for helping me to understand and frame the argument in these two paragraphs.

holders, not the Cloud providers. Encryption would also allow for greater protection of user privacy and give users greater control over their own personal data. One might hope that the widespread use of strong encryption would give users some capacity to push back against the ability of Cloud service providers to monitor and control content by preserving their autonomy and providing some cover for certain kinds of unwanted behavior.

Especially as regards privacy, one might hope that users might be able to successfully hide their content, even that stored on the Cloud, from peering eyes. In any event, encryption does not yet address the fundamental question of the power imbalance in the Cloud's architecture created by walled gardens, tethered thin-client devices and non-interoperable systems. As encryption is not always formally integrated or "baked in" to the architecture of the Cloud, users face significant usability, functionality, and capacity issues in order to use encryption technologies. The move towards thin-client "terminality" and away from user autonomy and computer power is primarily one of structure, not content; a problem which encryption only partially addresses.

## V. A Continued Movement Towards Greater Control, or a Quantum Leap?

I have dubbed this idea of the Cloud having the potential to become a closed, hierarchical space as a "third enclosure movement," following those enclosure movements previously identified by Polanyi and Boyle. Why not simply Enclosure 2.1, or 2.2? After all, Larry Ellison of Oracle has famously quipped that the Cloud is nothing more than what is already on offer on the Internet.[59] If so, increased control over content, better "locks," etc. is simply part of the normal evolution of the Internet.

The reason, in my view, why we are facing Enclosure 3.0 and not merely 2.1 or 2.2, lies in the substantial change in architecture. While it is true that to some extent the movement of copyright holders to emphasize (and perhaps over-emphasize) their rights continues unbroken into Cloud space, it is perhaps more relevant that the architecture has changed. Even with the various initiatives and strategies designed to enhance owner's rights—the WIPO Treaties, the DMCA, TPMs, the ACTA, and the HADOPI—it is still the case that all these measures meant to prevent digital copying could ultimately be circumvented; most colorfully by hacking, but most basically, one could always make an analog copy and then re-digitize it without TPMs. It is arguable that the structure of the Cloud makes control over content possible to a degree unmatched by these various legal measures. It is a paradigm shift in terms of control. Thus, the third enclosure movement might achieve total control, which would be impossible under Enclosure 2.0.

This is the uniquely new fear: that we lose the means to shape and adapt the technology to create both new technologies and new art forms, even where (especially where) the practice

[59] Larry Ellison, *What The Hell Is Cloud Computing?* YOUTUBE (October 10, 2012, 1:45 PM), http://www.youtube.com/watch?v=0FacYAI6DY0; *but see* Chris Kanaracus, *Ellison: Oracle Will Deliver World's 'Most Comprehensive Cloud'*, COMPUTERWORLD (June 6, 2012), http://www.computerworld.com/s/article/9227837/Ellison_Oracle_will_deliver_world_s_most_comprehensive_cloud_.

might be subversive, or constitute "piracy."[60] Put bluntly, we lose the ability to ethically participate, download, share, program, create, and, at times, hack. We become addicted to the "stream" until what we are being fed is ultimately turned off, or altered.

Architecture is important. The original motto of the Electronic Frontier Foundation, a slogan attributed to Mitch Kapoor, was "architecture is politics"; this motto then evolved to the less challenging "architecture is policy." With Lawrence Lessig, I prefer the original term.[61] Politics of the Internet space are changing fundamentally with the move towards Cloud space. The initial anarchy and disorganized democracy of the Internet is an ethic that has spawned both creativity and revolutions, whose political impact was tied in a fundamental way to its architecture. The worry is that a change in the Cloud's architecture will also change its politics.

The presence of the technology of the Cloud in and of itself does not lead to evisceration of the Internet. The Internet as the basic layer of communication among computers and servers will not disappear overnight and indeed to some extent will continue to exist and be used. Nevertheless, as more and more services immigrate to the Cloud and as Cloud services generally become more popular, the Internet may become feebler in what services it can provide vis-à-vis the Cloud. As

[60] For takes on the positive role of pirates and piracy, see ADRIAN JOHNS, PIRACY: THE INTELLECTUAL PROPERTY WARS FROM GUTENBERG TO GATES (2009). A similar argument has been made in the larger context of property reform. *See* EDUARDO M. PEÑALVER & SONIA K. KATYAL, PROPERTY OUT-LAWS: HOW SQUATTERS, PIRATES AND PROTESTERS IMPROVE THE LAW OF OWNERSHIP (2010); *see also* JULIE COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE AND THE PLAY OF EVERYDAY PRACTICE 187 (2012).
[61] LESSIG, *supra* note 12, at 243 n.19.

such, the Internet might become a second-rate place to interact and indeed may fail to keep up in terms of technological advances with the cutting-edge Cloud. So it is not enough to say that even if we can't access the closed Cloud, we can still access the Internet: much will have been lost. Cloud service providers are accelerating this shift by providing services at low or no cost, thereby enticing users into buying into their services: a "bait & hook" business model created by the desire of early players in Cloud service to acquire as much of this competitive market as possible at the outset. At some point, when these services have become popular (indeed, a large number of users have become reliant on them), these users may become extremely vulnerable to the power of the Cloud service providers which may then price discriminate or otherwise unilaterally alter the kinds of services provided or their levels. At this point, consumers have little choice but to accept the new terms or, if feasible, find an alternative service.[62]

Cloud technology presents enormous possibilities provided that we continue to share these computational resources and allow content to flow freely. Rather, it is the concentration of powers of the Cloud in the hands of the few and increased control over content, coupled with the relative weakening of the means of interaction with the Internet, that creates the power imbalance of the Cloud. Unless we can maintain some elements of the original Internet—its horizontality, its creative anarchy, its ethos of sharing—we

[62] A recent non-Cloud example is Google hiking the price to businesses for its Google Maps service. *See* Josh Costine, *Why Google's Plan To Make Maps Pay For Itself Could Backfire*, TECHCRUNCH (Mar. 9, 2012), http://techcrunch.com/2012/03/09/google-maps-api-vs-openstreetmap/. I thank Dan Grecu for this example and helping me to hone this analysis.

might be rendered powerless. The fear is that, in this digital sky, users move from sharing to being sheared.

## VI. AVOIDING ENCLOSURE 3.0

I do not wish to engage in an exercise of fear mongering simply for its own sake. None of this forecast is inevitable. We are still in the realm of the first and second Webs, with movement towards the Cloud being touted mainly as a way to efficiently and cheaply maximize storage capacity. If we keep an eye on preserving our computing power "on the ground" at myriad points, we might still maintain some of the horizontal nature of the Internet and even exploit the Cloud as we want to exploit it. The question then becomes how to tap into the positive possibilities of the Cloud without allowing digital fences to shut users out. What follows is a necessarily speculative list of suggestions.

Privately owned service providers provide Internet and Cloud services on the basis of contracts in the form of end-user licenses and subscriptions, and given this bargaining power they can dictate the terms of access. On a policy level, we might make alternatives for Cloud computing possible by fostering healthy competition through the mechanism of competition-anti-trust norms.[63] Consumer protection law is another legal regime that can be brought to the service of ensuring openness, interoperability, and portability of data (for example, when users change Cloud service providers), as well as ensuring that the contracts used to regulate Cloud-service agreements are even-handed. One might also employ user's bills of rights, consumer protection statutes, and privacy

[63] SLUIJS ET AL., *supra* note 31, at 15–26.

legislation to ensure that the gateway to the Cloud is an entrance point and not a barrier, and that individual information is protected in the digital sky. Setting minimum standards for both architecture and the contractual terms of engagement, if you will, would be a good step in creating a more accessible and open Cloud. All policy efforts and incentives should be considered to entice Cloud providers to not build private gardens by employing non-interoperable, proprietary platforms, but rather to strive for interoperability and open software platforms. A more radical solution might be to encourage or, if necessary, force such providers to maintain some small percentage of their private resources as openly available access points to their Clouds. Of course, this latter option, if not voluntary, would necessitate a direct form of government control which would be resisted in some quarters, as well as requiring a level of coordination among governments that thus far has proved difficult to achieve.

One must, however, remain sanguine about the ability of the privately held Cloud to be regulated. Given the power of the private actors involved and the realities of government capture in many countries (especially in the United States) we cannot guarantee that this form of privately delivered Cloud space can escape the vicissitudes identified above. We have thus far not been able to prevent private actors from creating incompatible formats in their hardware and software: we had not convinced Steve Jobs to envisage Apple as a more open platform for computing, as Blu-ray fans will know.[64] More

[64] Apple products, even those recent versions released shortly before Steven Jobs's passing, did not incorporate a Blu-ray compatibility, forcing Mac users to have to use additional software and hardware to try to play Blu-ray. *See, e.g.*, Darren Murph, *Apple's Steve Jobs Calls Blu-ray "a Bag of Hurt*", ENGADGET (Oct. 14, 2008, 1:57 PM),

importantly, we have failed in preventing the use of restrictive adhesion contracts and digital locks to lock up content, regardless of their flouting of copyright rules and principles and their impact on the public domain, and we have been equally ineffective in preventing the spread of norms, like the DMCA and InfoSoc Directive, that legitimize such practices. What James Boyle predicted in his employing of the enclosure metaphor is coming to pass at the level of formal law (even if such measures have yet to clearly succeed in practice). What was ironic about the anti-SOPA campaign was that it was directed by Google and Amazon;[65] how will they react when they are pushing against users and government legislation whose aim is to keep their systems open? Thus far, even though we may question some of its policies, Google has been a leader in promoting an open Internet, and so this is a source of optimism.[66]

http://www.engadget.com/2008/10/14/steve-jobs-calls-blu-ray-a-bag-of-hurt/; Geoffrey Goetz, *Tasting the Forbidden Fruit: Blu-ray on the Mac* GIGAOM (Jan. 7, 2011, 9:30 AM), http://gigaom.com/apple/tasting-the-forbidden-fruit-blu-ray-on-the-mac/.

[65] *See, e.g.*, Declan McCullagh, *Anti-SOPA Forces Have ISP Snooping Bill in Their Crosshairs*, CNET (Jan. 17, 2012) (explaining the role of large Internet companies like Google and Amazon in resisting the ultimately unsuccessful Stop Online Privacy Act (SOPA) copyright reform effort in early 2012).

[66] *See* Ian Katz, *Web Freedom Faces Greatest Threat Ever, Warns Google's Sergey Brin*, GUARDIAN, Apr. 15, 2012, http://www.guardian.co.uk/technology/2012/apr/15/web-freedom-threat-google-brin. Here too, there is more than a touch of irony: Apple's business model is predicated on non-interoperability of its hardware and to a lessening extent its software, while Facebook's is based on a walled garden. Google's business model is predicated on being able to search every corner of the Web and to gather information there. It is thus easier to cast its lot in favor of Web freedom. The question remains, however, whether Google is

While all of these options are highly desirable, they may be less effective than simply being vigilant about maintaining, on a local or national level, our own capacity to interact with technology through the development and maintenance of the publicly owned Cloud. This public capacity exists. Universities and government agencies could be employed, consistent with their vocation, to ensure that Internet and Cloud access (for both storage and computing) remains open.

It might also be achieved by tapping into the very strong open-source, open-access movements. The first Internet has demonstrated beyond a doubt the willingness of people to collaborate in building common, open, and accessible systems and platforms, for example, easy-to-use Linux distributions such as Ubuntu or Linux Mint, as well as substantive content bases and pools of knowledge—wikis and creative commons. This commitment by community groups will hopefully transpose itself onto the Cloud. By providing some measure of publicly delivered Cloud space, these kinds of movements might successfully continue. An example of such a community-based Cloud service is Ubuntu's Cloud, Ubuntu One, which uses space on Amazon's S3 Cloud.[67] These

benevolently fighting for users' rights or whether it is seeking to protect its own business model.

[67] *See* UBUNTU ONE, https://one.ubuntu.com (last visited Oct. 12, 2012); *Technical Details*, UBUNTU ONE, https://wiki.ubuntu.com/UbuntuOne/TechnicalDetails (last visited Oct 12, 2012). Canonical Ltd runs the Cloud service and draws revenue from paying users, but it is the Ubuntu community that uploads patches and makes supported applications. Most users at this stage do not need to use more than the free 5GB, a quantity that was increased from 2GB in July 2011.

movements provide the greatest source of hope for creating and better defining[68] the community Cloud.

It is obvious that I am following the line of thought that emerges from the belief, with Boyle, Litman, Lange, and others, in the need to protect the public domain of ideas from the encroachment of the private. This is especially true in the realm of copyright, but is also true in other areas of intellectual property. But I would hasten to add that the position of reinforcing directly the publicly held Cloud (and indirectly encouraging the privately held Cloud to remain open) is also predicated on the virtue of sharing content and its maintenance as the ethical barometer for Internet practice and structure. Sharing not only reinforces the exchange of ideas, information, and knowledge, but also requires a certain kind of ethical stance based on horizontal interconnection, responsibility, and development of knowledge.

It is equally obvious that I am following a line of argument in which knowledge and know-how generally form part of an intellectual commons.[69] This applies both to content (i.e., knowledge as a resource) and the infrastructure that makes it possible. Charlotte Hess and Noble Laureate Elinor Ostrom have characterized knowledge as an intangible, pure public (i.e., non-exclusive and non-rivalrous) good[70] and as a

[68] Answering the concern that "community Cloud" is "ill defined" in Kushida et al., *supra* note 37, at 234.

[69] *See generally* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990); UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE (Charlotte Hess & Elinor Ostrom eds., 2007).

[70] Charlotte Hess & Elinor Ostrom, *Introduction*, *in* UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE, *supra* note 69, at 9.

"flow resource," a resource whose value lies in its circulation among people.[71] Thus not only does the content of the public domain of ideas form a static part of the pool of knowledge, but rather it derives its value from flowing among people, being communicated, transmitted, imparted, or otherwise shared.

In this sense, the Internet and the Cloud in terms of structure and content are part of the acquired knowledge of a society and thus can be treated as a kind of digital commons or common good; it is to be open and able to be shared by all. The architecture of the Internet and Cloud is thus a *bien commun*.[72] The notion of a commons can be effectively maintained over time, as Ostrom has pointed out, but it requires active management.[73]

[71] Charlotte Hess & Elinor Ostrom, *A Framework for Analyzing the Knowledge Commons*, *in* UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE, *supra* note 69, at 48–49, 53.

[72] I am haunted by a comment made by Gianfranco de Bertolini, based on Foucault: maybe all that the move to the Cloud has done is to point out that we never really had the power in the Internet that we thought we did have. Other hidden forces had it, and exercised it, without being seen or noticed. The Cloud has simply brought theses forces out into the open. In my view, there is no question that, as architecture is politics, political forces have been at play since the inception of the Internet. For the time being, I remain convinced by the analysis that the first Internet was meant to be based, and was based in practice, on a series of assumptions that were open and not completely controllable.

[73] OSTROM, *supra* note 69, at 90–102. To be more precise, in order for collective management of common-pool resources institutions to remain stable over the long term and succeed, Ostrom's empirical study found that they has to exhibit the following design characteristics: (1) clearly defined boundaries needed to be in place; (2) rules needed to be matched to local needs and conditions; (3) individuals affected by these rules could usually participate in modifying them; (4) community members have the right to

An equally sophisticated argument can be made for the idea that the *infrastructure* of the knowledge commons (an infrastructure that would include the Internet and the Cloud) also forms part of the intellectual commons. In this regard I am following Brett Frischmann, who argues that "intellectual infrastructure" exhibits the characteristics of other infrastructures, and the Internet is an example of an "infrastructure commons."[74] These digital infrastructures are valuable as a shared resource that in turn makes other kinds of important and essential activity—creative, communicative, economic, and otherwise—possible. As such they are similar to roads and railways, typical examples of public goods. These commons need to be managed.[75]

An aspect of this larger knowledge commons is the "innovation commons," the ability to use the current state of knowledge to innovate and create in an unhindered and

devise their own rules and these rules are then respected by external authorities; (5) an established system of self-monitoring of member behavior; (6) a graduated system of sanctions exists (7) community members can resolves disputes at low cost; and (8) the governance activities regarding the resource are organized in a multiple layered, "nested" structure.

[74] *See generally* FRISCHMANN, *supra* note 14, at 253–316.

[75] According to Frischmann, regarding the management of the infrastructure commons, "commons management is a functional concept that describes the situation in which a resources is shared among members of a community on nondiscriminatory terms. In general, *nondiscriminatory terms are terms that do not depend on the users' identity or intended use.* Members of the community have equal opportunities to use the resource as they see fit, under conditions that are more or less uniform. Users decide what to do, with whom to interact, or how to use the shared resource; their choices are not predetermined or prioritized by the terms or conditions set by infrastructure providers. This does not mean that use of the resource is free or comes without any terms and conditions." *Id.* at 92.

uninhibited way.[76] However, innovation remains only an aspect, and many of the other ways in which this infrastructure is used (communication, for example) are not necessarily innovative.

The key feature of the infrastructure commons that we have come to know as the Internet is the end-to-end architecture described above. It is, according to Frischmann, the interaction among end users that has generated the vast benefits that we have seen with the Internet:

> The benefits of the Internet are generated at the ends. Like a road system, a telecommunications network, an ocean, and basic research, the Internet is socially valuable primarily because of the wide variety of productive activities that it facilitates. End-users generate value and realize benefits through their activities, which involve running applications on their computers; generating, consuming and using content; and creating and engaging in various social, economic, or other relations with other users. . . . Keep in mind that *activities on the Internet* always involve *interactions* among *end-users*; that the interactions may be commercial, educational, social, political, and so on; and that end-users may be individuals, corporations, government actors, or other entities.[77]

I would add that this interaction must include the possibility of "generative" interaction in Zittrain's terms. It is

[76] *See generally* LESSIG, *supra* note 12; FRISCHMANN, *supra* note 14, at 333.
[77] FRISCHMANN, *supra* note 14, at 334.

this user interaction that we must seek to maintain in choosing governance structures as we move to the Cloud.

Hence, moving from the Internet to the Cloud, it is my view that some sort of public management or oversight might be required. Frischmann has identified good reasons as to why private owners should adopt a commons-management strategy as regards the Internet, in particular favoring the "end-to-end" design: (1) consumers generally dislike discrimination; (2) ease and lower cost of management; (3) facilitation of joint production and cooperation; (4) support value creation by users; and (5) flexibility in the face of uncertainty.[78] An "astounding number" of networks run by private and public entities choose this strategy.[79]

However, as seen in the discussion of base metaphors above, the architecture of the Cloud allows for a possible rejection of the fundamental "end-to-end" principle, by allowing for increased control, vertical integration, and potentially successful closed business models. Indeed, it may very well be that this basic principle is under stress already, with pressures on Internet service providers to move away from Internet neutrality by traffic shaping, throttling, and such. These architectural changes behind the move to the Cloud fit well with the factors that Frischmann identifies for rejecting a commons management strategy:

> [P]rivate infrastructure owners have a number of reasons for choosing to reject a commons management strategy, such as opportunities to price discriminate, vertically integrate and

[78] *Id.* at 345–46.
[79] *Id.*

> operate for a subset of downstream markets, and control future progress.[80]

This is precisely the fear for which I am trying to raise awareness: the potential for control on the part of Cloud providers (and, I suppose, the potential for increased profits) through a vertical model, thin clients, walled gardens, etc. lessens the incentive for them to opt for commons management schemes.

Frischmann's solution for the Internet is that it be managed as a "mixed infrastructure," in effect paralleling the "mixed semi-commons"—mixtures of private rights and commons—created by intellectual property regimes as regards the state of knowledge, art, and science.[81] I agree that this governance norm should also extend to the Cloud as well, if we are to realize the Cloud's potential and continue with it along the lines of the Internet as a shared resource. So while private actors will form part of the solution to the challenge of keeping the Cloud open and nondiscriminatory, we must admit that the public sector will also have to play a regulatory role in ensuring that private actors on the Cloud remain in line with the open, commons-management model, and in all likelihood may even have to enter the fray directly by providing infrastructure.[82]

[80] *Id.* at 347, 91–116.
[81] *Id.* at 301–14.
[82] Frischmann identifies four primary types of government intervention: (1) public regulation of private infrastructure providers mandating non-discriminatory access for competitors; (2) public regulation of private infrastructure providers mandating non-discriminatory access for consumers; (3) dedication of privately produced infrastructure to the public domain; and (4) public provision of infrastructure on a non-discriminatory

So we must also be open to the possibility of the need to create a publicly delivered Cloud to allow access to those who either cannot afford to use the privately held public Cloud or who may not wish to participate under restrictive terms (or run the risk that they will become too restrictive). It would also give a voice to those who wish to maintain the various open software and public domain projects seen thus far on the Internet. As such, a publicly held Cloud does not have to be a massive investment in infrastructure. It is perhaps ironic, however, that the most important function of maintaining some sort of publicly held Cloud, even if only a small one, is the positive impact that it will have on the *privately held* Cloud. A Cloud that is open, inexpensive, flexible, and secure is in effect a competitor in providing services on the publicly held part of the Cloud and will hopefully encourage similar features throughout the Cloud.[83]

For the time being, in skeletal form, I would argue that the publicly held Cloud needs to be created, bolstered, and maintained by:

basis. *Id*. at 100. It is also interesting to note the fears that I have identified as regards the structure of the Cloud would also cohere with the necessary prerequisites for judicial intervention imposing obligations of equal and nondiscriminatory access under antitrust law in the United States, using the "essential facilities doctrine," as identified by Frischmann: (1) a monopolist controls access to an essential facility; (2) the facility cannot be reasonably duplicated by a competitor; (3) the monopolist denies access to a competitor; and (4) it was feasible to grant access. *Id*. at 101–02. Should the market situation reach this point as among Cloud providers, this doctrine could very well be employed. It would be wiser to use legislative, regulatory, and persuasive means to not reach this point.

[83] Moving even further in this sense, again ironic, such a public venture need not be all that directly successful. It is there in case the taps get turned off, and it is successful indirectly where the private projects succeed.

- providing resources to public actors (like universities) for building the computing and storage infrastructure to create and maintain a minimal, publicly delivered Cloud service;

- encouraging open software, open access, open knowledge and digital sharing movements to continue; and to provide Cloud services where possible;

- where necessary, encouraging or forcing universities and other agencies funded by the state to maintain a Cloud, providing the various kinds of Cloud services (SaaS, IaaS, PaaS) directly to not only their staff and students, but to the wider community and community Clouds; and

- perhaps using public-private partnerships (PPPs).

Admittedly, this last scenario is a more challenging option but might nevertheless be appropriate in those contexts where states do not have the capacities in their public institutions to provide Internet and Cloud services. It may also be the case, as has been the case in the varied contexts and economic histories of many countries, that the *quango* (or quasi-autonomous state agency, Crown corporation, etc.) is the appropriate tool for the development of this critical resource. No good idea for a hybrid solution should be rejected *a priori*. Different countries might find different solutions depending on their policy contexts.

Moreover, I would argue that governments need to ensure that the privately held Cloud *remains* accessible by:

- mandating and implementing the highest standards of interoperability in Cloud technology, encouraging the use of open platforms and open access software, and barring attempts by individual providers to lock their systems;

- protecting users from monopolistic business practices through competition and consumer law;

- requiring privately delivered Cloud service providers to make space available to community Clouds and community-driven projects such as Ubuntu One;

- mandating and implementing the highest privacy standards, perhaps via a user's bill of rights;[84] and

- mandating the highest standard of basic user rights, again perhaps via a user's bill of rights.

Further, as far as possible, it would be beneficial to make the privately held Cloud conform to these last desiderata, either through positive legislation or incentives.

As regards the architecture of the publicly held Cloud, the availability of resources (human know-how, physical infrastructure, and ongoing financial resources) is necessary.

[84] For an example of such a movement, see Internet Rights & Principles Coal., IRP CHARTER, http://irpcharter.org/charter/ (last visited May 30, 2012).

The key may very well be in “reminding” universities and public research centers of their public vocation, which in Europe, Canada, and the United States could work effectively, provided that the resources to maintain the public Cloud are indeed furnished. But the use of universities, for example, does not preclude other *loci* for the provision of cloud computing capacities. Collaborations among governments, say the European Union and Canada, for example, might be encouraged to build facilities—built and perhaps operated jointly—in northern climates that are both cold enough to cool the physical infrastructure supporting the Cloud and close to clean sources of electricity; resources currently necessitated by Cloud server technology.

I am aware that governments have not always been the most virtuous players on the Internet. They have blocked access to the Internet and its content, and even governments generally considered to be “responsible” and “democratic” have used it for surveillance purposes. Indeed, in some places it is clear that governments ought best be feared. Hence, there is also a serious, related concern with the possibility that governments may use the potential controllability of the Cloud as an efficient means to gather information about individual users for a variety of purposes. Acknowledging this fact, I would still maintain that collaboration between accountable governments and government institutions, on their own or with the private sector, could set a high ethical standard for Internet and Cloud participation.

Thus, in the end, polycentric solutions—private, directly provided government services, and indirectly “government-encouraged” services by public, quasi-public and even private actors—will form a part of the mix in keeping the Cloud’s gates from being controlled by private Cerberus. Of course this means that governments will need to take a proactive role domestically, and cooperate at an international level. But hopefully even the most minimalist political ideology will (1) see the importance of this role for the development of its own citizenry and economy, and (2) find within the various governance options ones that it can implement according to its own philosophy.

## VII. CONCLUSION

One of the ironies of Lon Fuller's great book, *The Morality of Law,*[85] was that, having identified law's "morality of aspiration" in the first part of the book, the substantive contents of this aspirational morality nevertheless eluded him. The best that he could do was to set out a list of procedural desiderata that would help ensure that law's morality of aspiration, indeed its morality *tout court*, would flourish. The same kind of irony is present in this case as well. If we take care of the Cloud in an almost procedural manner by ensuring access to its capacities and by providing an open set of protocols underlying it, then the substantive Cloud (or content on the Cloud) will flourish just as it did with the original Internet.

Indeed, Fuller went even further, and was unwittingly prescient on a matter that would arise a half-century after he wrote his book. Regarding the morality of aspiration, when asked to identify one "indisputable" principle of natural law, Fuller fixed upon the creation and the maintenance of channels of communication "by which men convey to one another what they perceive, feel, and desire":

[85] LON L. FULLER, THE MORALITY OF LAW (1964).

> [I]f we were forced to select the principle that supports and infuses all human aspiration we would find it in the maintaining communication with our fellows. . . . Communication is something more than a means of staying alive. It is a way of being alive.[86]

By focusing on architecture and access, we will encourage the continued explosion of creative capacities, and the continued sharing of knowledge and information that has characterized the Internet. Perhaps on this Cloud sheep can fly. But they'll need some help.

[86] *Id*. at 185. I thank Kevin Gray for reminding me of just how far Fuller went on this point. Indeed, these same passages from Fuller are originally cited by Gray to support the idea that some resources were morally *non-excludable*—and therefore outside of private property regimes—in the thoughtful and provocative article: Kevin Gray, *Property in Thin Air*, 50 CAMBRIDGE L.J. 252, 281 n.46 (1991). Current theorists of the public domain/commons should take note. As I have argued elsewhere, property objects or resources shape the possible panoply of property relations, public and private. *See* David Lametti, *The Concept of Property: Relations Through Objects of Social Wealth*, 53 U. TORONTO L.J. 325 (2003); and David Lametti, *The Objects of Virtue, in* PROPERTY AND COMMUNITY 1 (Gregory S. Alexander & Eduardo Peñalver eds., 2010).