CLOUD CONTROL: COPYRIGHT, GLOBAL MEMES AND PRIVACY

DANIEL J. GERVAIS & DANIEL J. HYNDMAN*

> Imagine for a moment that electricity was used only to power one kind of computer known as an *electricity computer*. That is what computer power is like now: it mainly powers devices that sit on our desks with qwerty keyboards attached. As computing becomes a utility it will power many more devices, many of them with no user interface, more of them mobile and handheld. The Cloud should also encourage collaboration. Different people, using different devices should be able to access the same documents and resources more easily.[1]

* Daniel J. Gervais is Professor of Law and Co-Director of the Technology and Entertainment Law Program at Vanderbilt University Law School. Daniel J. Hyndman, J.D., Vanderbilt University Law School Class of 2011.

1. CHARLES LEADBEATER, CLOUD CULTURE 29 (2010).

INTRODUCTION

iTunes' Match service scans a user's computer to determine which music is there and then gives that user access to the same music (though contained in different, "clean" files) on its Cloud.[2] In that process iTunes matches song titles with those in its database, but reportedly it can also determine whether each song on the user's computer was originally an iTunes download, ripped from a CD or acquired (presumably illegally) via peer-to-peer (p2p) networks.[3] If and when this occurs, a list is generated on Apple's servers matching the user's iTunes account with a specific number of p2p acquired songs. What would prevent record companies from subpoenaing that list and suing the account holder for $150,000 per song, the maximum amount of statutory damages allowed under the US Copyright Act?[4] The user's privacy interests are unlikely to stand in the way, as we demonstrate in this Article. In fact, record companies may not even have to notify a user that they are asking for access to those files. They would have to notify Apple, of course. However, other than the very real possibility that the rule against fishing expeditions would apply, it might in fact be hard for Apple to make a case against the subpoena.[5]

This scenario is one of many such examples because soon everything digital will be in the Cloud, including our personal data. Almost every bit of human culture, every song, book, document, and movie ever made. Then everything about us: banking and tax information, online purchase history, Facebook posts, Tweets, pictures, and even a full backup of our personal files—and eventually the files themselves.[6] This portentous change will have significant advantages,

---

2. *See* iCloud, APPLE.COM, http://www.apple.com/icloud/features (last visited Nov. 19, 2011).

3. *See* Mike Masnick, *Forget Laundering Unauthorized Music Via Music Match, What About AirDrop Darknets?*, TECHDIRT (June 7, 2011), http://www.techdirt.com/articles/20110606/20285814570/forget-laundering-unauthorized-music-via-music-match-what-about-airdrop-darknets.shtml.

4. Copyright Act, 17 U.S.C. § 504(c)(2) (2010). One might legitimately ask why record companies would license Apple to do all of this "cleaning" for a mere $25. *See id.* Can it be said that Apple is encouraging a pre-cleaning p2p bonanza so that more files will be cleaned? Let us push the scenario one step further. If file-sharing is made a felony, as proposed in bills pending as of this writing, would it be possible to make a conspiracy case against Apple? *See* Commercial Felony Streaming Act, S. 978, 112th Cong. (2011); Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011). It is not clear that the bills will pass, of course. A similar attempt failed in 2003. *See* Jay Lyman, *New Bill Makes File Swapping a Felony*, TECHNEWSWORLD (July 7, 2003), www.technewsworld.com/story/31138.html.

5. *See, e.g.*, Julie Samuels, *Judge Shuts Down Another Mass Copyright Case, Characterizes Lawsuits as "Massive Collection Scheme"*, ELECTRONIC FRONTIER FOUNDATION (Sept. 8, 2011), http://www.eff.org/deeplinks/2011/09/judge-shuts-down-another-mass-copyright-case.

6. Access to media on the Cloud, particularly music, has become one of the most

such as access to all those resources much more easily and on any digital device, an approach illustrated by Apple's recent platform paradigm uniting all Apple devices belonging to the same user.[7] The Cloud will not replace personal storage but it will reduce the (perceived) need to keep individual copies and thus serve as a general depository for both commercial and private content, and of course all kinds of admixtures of both, most notably to create "user-generated content."[8]

The Internet itself was a major shift from a central or mainframe architecture to a client-server architecture. Pre-Cloud, the Internet was used to transport data and allow hundreds of millions of individual and corporate computers on which content was stored to exchange using their Internet identity (an IP address).[9] Switching from this *connection paradigm*, in which the Internet was essentially a network connecting computers, to an *amalgamation paradigm*, where user computers and devices are merely tools used to access private and commercial content amalgamated on server farms operated by major intermediaries, is not a

---

popular uses among normal users. Services like iTunes (www.apple.com/itunes) allow for users to pick and choose which tracks they want to buy and download, while Grooveshark (www.grooveshark.com) allows for direct streaming of many tracks directly from the user's Internet browser. Most banks have their own sites for online banking (for example, www.bankofamerica.com), and now users can monitor personal finances in the Cloud using something like Mint (www.mint.com). Amazon (www.amazon.com) keeps track of your purchases and uses that information to make recommendations on other things you might like. In the social part of the Cloud, Facebook (www.facebook.com) is perhaps the most important player, but simple services like Twitter (www.twitter.com) are increasing in popularity if they are able to find the right niche to fill. Google (www.google.com) has a wide variety of ways to store personal media in the Cloud and share it with others, including YouTube (www.youtube.com) for videos and Picasa (picasa.google.com) for photos. Dropbox (www.dropbox.com) offers a service that allows users to store their files online so they can be accessed anywhere while behaving as just another part of the user's hard drive to create a seamless integration of the home computer and the Cloud.

7. Apple's (www.apple.com) push for unifying the use of all its products into one experience reflects their general attempt at providing a simple-to-use experience without requiring a lot of computer knowledge. When the iPod first appeared, it was a simple, but revolutionary, mp3 player. Now, the iPod can access the Internet to synchronize with the user's iTunes profile, allowing access to a lot of music at any time. The iPhone contains a lot of similar functionality. The iPad, Apple's newest gadget, seems to bridge the gap between a smart phone and a netbook, allowing users to do many of the things they would do on a computer, but through the touch screen interface similar to the iPhone. All of these products use Internet access to sync with the user's media and data they have stored in the Cloud, unifying the user's experience.

8. *See* Paul Resnikoff, *The Cloud: It's Not an Evolution . . .*, DIGITAL MUSIC NEWS (Mar. 2, 2011), http://www.digitalmusicnews.com/stories/030211Cloud?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+digitalmusicnews+%28Digital+Music+News%3A+Top+Stories%29.

9. This is usually described as the Transport Layer and the Internet Layer. *See* NICHOLAS CARR, THE BIG SWITCH: REWIRING THE WORLD, FROM EDISON TO GOOGLE 54–55 (2008).

benign change.[10] One can easily delete a file on one's computer and overwrite the old file location to make the data unrecoverable.[11] Will it be possible to completely delete information uploaded to the Cloud? If not, do we still *own* information we upload to the Cloud?[12] How will privacy be protected when every bit of information and every bit of digital content belonging to each one of us resides on the same servers? Will major content providers such as record labels and film studios gain greater control on how we access and use commercial copyrighted content? Who will have *jurisdiction* over the Cloud? If countries adopt different jurisdictional tests (headquarters of Cloud operator, location of servers, etc.) conflicts and uncertainty are just around the corner.

In this Article, we tackle two of the most important questions raised by the emergence of the Cloud: privacy and copyright. In both cases, we have tried to identify how the application of extant rules may be altered by the architecture of the Cloud. Then we consider ways to ameliorate those rules to avoid some of the most problematic aspects of the move to the Cloud. Accordingly, after defining the "Cloud" in Part I, in Part II we consider copyright and related cultural issues, in particular access to and control of culture. Part III presents the challenges for privacy protection in the Cloud, and Part IV suggests reforms to privacy law and policy.

I. DEFINING CLOUD COMPUTING

A. A New Global Infrastructure

Cloud computing is a term used to describe a *global technological infrastructure* in which the user of a computer accesses and uses software and data located outside of the user's personal computer or other digital device.[13] The user connects to these external devices by way of an Internet connection, but typically has no knowledge of the nature or even location of the server on which the data and software are located. This anonymous, external, and often unidentifiable interaction is known as "cloud computing" or simply "the Cloud."[14]

---

10. *See supra* text accompanying note 6.

11. One could also physically destroy the medium, of course.

12. The right to destroy one's own property goes back as far as Roman law, though it has had its detractors, including John Locke to some extent. It is an extension of the right to exclude, in that it effectively excludes everyone, including the owner, from use at any time in the future. The extent to which this applies to electronic data has not been decided though the value of personal data to society seems minimal and as such, people should be allowed to destroy it as they see fit. The question still remains as to whether a user still owns data that they've put in the Cloud. *See generally* Lior Jacob Strahilevitz, *The Right to Destroy*, 114 YALE L.J. 781 (2005).

13. *Battle of the Clouds*, ECONOMIST, Oct. 15, 2009, at 16, *available at* http://www.economist.com/node/14644393.

14. *See* JOTHY ROSENBERG & ARTHUR MATEOS, THE CLOUD AT YOUR SERVICE 1–3

As already noted, this is not a benign change. Before the advent of Cloud computing, users mostly ran software and processed data on their own personal computer. The Internet was used to transmit processed data between two or more computers.[15] In contrast, with Cloud computing, the user stores (uploads) and accesses (downloads) data located on external computers that the user does not own, does not control, and cannot locate. She only knows (hopefully) which entity ostensibly provides access to the service, whether it be storage (backup), data processing (access to a program), or both.[16]

One of the main reasons for the rise in popularity of Cloud computing has been the increase in Internet download and upload speeds.[17] The use of the Cloud as a backup storage facility is only practical if it is possible to get large amounts of data transferred to the Cloud at reasonable speeds.[18] On the slow Internet connections that were available in the mid-1990s, it would simply not have been practicable to upload a large collection of files to a server over the Internet. The 56 kilobit/second modems of the 90's have given way to the much faster cable modems and other modern networking devices, offering speeds 1000 times faster or more.[19]

At some point in this progression of Internet speed, a threshold was crossed. It marked Internet users' ability to access services offered in the Cloud just as easily as running software on their computer.[20] The process began with relatively low bandwidth services that didn't require a constant flow of information, like email services that store the messages

---

(2010); Daniel Lyons, *Today's Forecast: Cloudy*, NEWSWEEK, Nov. 1, 2008, at 24, *available at* http://www.newsweek/id/166818.

15. Nelson Minar & Marc Hedlund, *Chapter 1: A Network of Peers: Peer-to-Peer Models Through the History of the Internet*, *in* PEER TO PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES 3, 3 (Andy Oram ed., 2001), *available at* http://oreilly.com/catalog/peertopeer/chapter/ch01.html (Chapter 1 contains a good basic description of the Peer-to-Peer Model and Client-Server Models).

16. *See id.* at 3-4; CARR, *supra* note 9.

17. Webmail services like Yahoo! Mail (http://mail.yahoo.com) could be used effectively even at dialup Internet speeds (maximum of 56 Kbps), but services like video streaming through Netflix (www.netflix.com) require some degree of broadband connection to be fully functional.

18. Arif Mohamed, *A History of Cloud Computing*, COMPUTERWEEKLY.COM (Mar. 27, 2009), http://www.computerweekly.com/Articles/2009/06/10/235429/A-history-of-cloud-computing.htm.

19. *Compare* FiOS Internet, VERIZON.COM, http://www22.verizon.com/Residential/Fiosinternet/#plans (last visited Nov. 19, 2011) (Verizon's fiber optics-based Internet that can deliver a maximum of 50 Mbit/s), *with* Minnie Ingersoll & James Kelly, *Think Big with a Gig: Our Experimental Fiber Network*, THE OFFICIAL GOOGLE BLOG (Feb. 10, 2010, 8:00 AM), http://googleblog.blogspot.com/2010/02/think-big-with-gig-our-experimental.html (Google's plan to begin offering 1 Gbit/s connections).

20. Mohamed, *supra* note 18.

on their own servers.[21] With recent ameliorations in bandwidth (broadband) availability, those services have expanded to the point of streaming high quality video and audio media directly over an Internet connection with little or no waiting time.[22] It seems reasonable to predict that as the network infrastructure becomes capable of providing new kinds of services and user experiences reliably, the Cloud will expand to new areas. The end game is probably one in which all digital content is either stored exclusively on, or at least backed up on, the Cloud.

Another important factor in the growth of Cloud computing has been the expansion in number and type of digital devices. In the early years of personal computing, a single computer was a luxury item, and few people owned more than one.[23] However, with advances in hardware design and the shrinking of processor chips,[24] it is now normal for a household to have multiple desktop computers. In parallel, portability increased (laptops), and small devices (phones) became more powerful and able to transmit and process digital data files.[25] The very existence and relative affordability (at least in industrialized countries) of these devices has created an enormous demand for services that can be used in a cross-platform way. This allows a user to check email, download and listen to music and movies, and watch YouTube videos whether the user is at home on his couch or riding a train to work.[26] Netbooks are perhaps not just a cause of Cloud computing but also an effect.[27] Many such devices take advantage of the fact that a lot of processing and storage of information is done on the Cloud. In fact, the rapid rise in computing

21. For example, YAHOO! (http://mail.yahoo.com), HOTMAIL (http://www.hotmail. com), and more recently GMAIL (http://mail.google.com/mail).

22. For example, NETFLIX (http://www.netflix.com).

23. Average personal computer prices fell below $1000 in November 1998. *See* Nancy Weil, *Average PC Price Drops Below $1000*, PC WORLD (Dec. 22, 1998), http://www.pcworld.com/article/9150/average_pc_price_drops_below_1000.html. In October 2009, the average price of portable Windows personal computers fell to $519. *See* Shane O'Neill, *Falling PC Prices Pit Microsoft Against PC Makers*, CIO.COM (Dec. 2, 2009), http://www.cio.com/article/509556/Falling_PC_Prices_Pit _Microsoft_Against_PC_Makers.

24. *See, e.g.*, Moore's Law, WIKPEDIA.COM, http://en.wikipedia.org/wiki/Moore%27s_law (last visited Dec. 24, 2011).

25. The current iteration of Apple's popular iPhone can be used to browse the Internet, run hundreds of different applications, and take and share photos and video. It even allows for live video chat between two devices. *See Apple – iPhone 4 – FaceTime, Retina Display, and More Features*, APPLE.COM, http://www.apple.com/iphone/features (last visited Nov. 19, 2011).

26. Cloud providers like Apple and Google have begun to provide nearly seamless experiences between various devices when it comes to accessing email, photos, or music, all of which are now easily stored in the cloud. *See* GMAIL, http://mail.google.com; ITUNES, http://www.apple.com/itunes; YOUTUBE, http://www.youtube.com.

27. A netbook is a personal computer that is meant to be smaller than modern laptops with an emphasis on battery life and portability. This is achieved by including smaller, less powerful components. A netbook relies on applications that can be run from the Internet in an Internet browser for most of its functionality, making it heavily reliant on the Cloud.

power may be slowed dramatically, as the focus shifts to smaller and less expensive devices.[28] By using the Cloud, netbook and phone manufacturers are able to use cheaper, smaller, less power-hungry hardware to create tiny devices with long battery life.[29]

Everyone is using the Cloud it seems, from the basic, casual user to the large corporation.[30] Casual users use Cloud computing to stay connected with their friends and to maintain a persistent presence on the Internet. Access to Facebook has connected millions of normal people who may have otherwise lost touch with each other or never met.[31] Digital stores allow users to shop easily from anywhere.[32] At the beginning of 2010, iTunes crossed the line of 10 billion songs sent to users.[33] Services like Steam allow users to purchase computer games that are then tied to an online account.[34] This allows users to access their account and games from any device without CDs or other forms of hardware media. In fact, the Cloud may just mark the end of the CD as a vehicle to sell software.[35] For casual users the Cloud is not just about media, however. There are myriad ways to use the Cloud for productive interaction. For example, Google Docs allows for sharing of documents, and multiple people can edit a document or spreadsheet.[36] More generally, the Cloud offers opportunities to share and transform content collaboratively thus offering new modes of expression for creativity.[37]

Companies use the Cloud for different purposes, as a way to increase the efficiency of their operations. For example, by storing files and using the Cloud's processing power, they avoid expensive investment in hardware.[38] Companies now pay for computing power and

---

28. *See, e.g.*, Yukari Iwatani Kane & Don Clark, *Apple's iPad Chalks Up Strong Sales in Weekend Debut*, WALL ST. J. ONLINE (Mar. 14, 2011), http://online.wsj.com/article/SB10001424052748704027504576198832667732862.html (iPad sales and projections).

29. For example, the low prices of netbooks. *See* Shane O'Niell, *Netbook Price War Could Hurt Microsoft*, PC WORLD (Apr. 14, 2009), http://www.pcworld.com/article/163095/netbook_price_war_could_hurt_microsoft.html.

30. Microsoft's push "to the Cloud" by providing Cloud services. *See* Cloud Power, MICROSOFT, http://www.microsoft.com/en-us/cloud/default.aspx?fbid=iqpEbSWZGHV (last visited Nov. 19, 2011).

31. *See* FACEBOOK, http://www.facebook.com (last visited Nov. 19, 2011).

32. *See, e.g.*, AMAZON, http://www.amazon.com (last visited Nov. 19, 2011).

33. Philip Elmer-Dewitt, *Apple iTunes: 10 Billion Songs Later*, CNN.COM (Feb. 24, 2010), http://tech.fortune.cnn.com/2010/02/24/apple-itunes-10-billion-songs-later.

34. *See* STEAM, http://store.steampowered.com (last visited Nov. 19, 2011).

35. Steam, an online video game vendor, is estimated to have sales of $1 billion in 2010. *See* Paul Tassi, *Steam Sales Estimated Close to $1 Billion in 2010*, FORBES.COM (Feb. 4, 2011), http://blogs.forbes.com/insertcoin/2011/02/04/steam-sales-close-to-1-billion-in-2010.

36. *See* GOOGLE DOCS, http://docs.google.com (last visited Nov. 19, 2011).

37. See Daniel Gervais, *The Tangled Web of UGC: Making Copyright Sense of User-Generated Content*, 11 VAND. J. ENT. & TECH. L. 841 (2009); William W. Fisher III, *The Implications for Law of User Innovation*, 94 MINN. L. REV. 1417 (2010).

38. CARR, *supra* note 9.

storage space as a utility.

B. NIST Definition

The National Institute of Science and Technology (NIST) has created a definition and description of the term "cloud computing," allowing for a more coherent conversation on the topic.[39] The definition states:

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[40]

NIST admits that, along with most topics regarding Cloud computing, this definition and the terms used are subject to rapid change due to the relatively recent explosion in advancement and popularity of the model. However, it does provide a jumping-off point for detailed discussion about the attributes, advantages, and disadvantages of Cloud computing. The five essential characteristics mentioned in the definition are:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service[41]

Let us look at each of these features briefly.

On-demand self-service defines the importance of automated access to the services and resources provided in the Cloud. The user needs to be able to interact with Cloud services without the need for a human intermediary. This factor is mostly taken for granted in the current state of the Internet. The convenience inherent in this factor is one of the most important requirements for a successful Cloud service.

Broad network access means that the service should be accessible across a variety of devices. This factor, like the previous one, is important but now mostly obvious. If a user's access to an email service

---

39. *See* PETER MELL & TIM GRANCE, NAT'L INST. OF STANDARDS & TECH. [hereinafter NIST], 15 THE NIST DEFINITION OF CLOUD COMPUTING (2009), http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

40. *Id.*

41. *Id.*

were limited to that user's home computer, it would be no different from the user simply downloading email and storing it on that computer. Part of the key of the success of Cloud services is their inter-operability with a variety of devices, using a cross-platform user interface.

Resource pooling is a characteristic that exists behind the scenes and is less obvious to users but no less important. It reflects the necessity of the Cloud service provider monitoring the use of computing resources and controlling the allocation of those resources. For instance, when a user uploads a video to YouTube, to some extent it appears one can upload an endless number of files. YouTube does not assign a hard drive or part of a specific server to a user. Videos are merely allocated a certain amount of space that exists in the provider's large pool of video storage space, known as a "server farm." It is up to the provider to properly and efficiently control the allocation of that storage pool. The user remains on the outside with no real knowledge of which particular physical resource he is using or accessing, including its actual location.

Rapid elasticity is related to resource pooling. While resource pooling is about abstracting the user away from knowledge of the resource used, rapid elasticity requires that the service provider be able to quickly handle changes in resource allocations. The provider must be able to scale up quickly to users' needs and scale down just as quickly to keep the maximum amount of resources free for use. In this way, the service provider retains what one might call the "Cloud effect," that is, keeping users insulated from knowledge of the behavior and limitations of the system's capabilities as much as possible.

Measured service is a factor that defines the interaction between user and provider. Allowing users to pay per unit of service is attractive in that it allows users to obtain up-to-date computer services without investing in new hardware and software. With a "measured service," companies or individuals can contract to get only the services they want or need.

The NIST Cloud computing definition also describes several service and deployment models which, for the most part, are beyond the scope of this paper. However, they highlight an important idea that resurfaces repeatedly, namely the Software as a Service (SaaS) model.[42] This model describes the interaction of most users with Cloud services. It is represented in many popular websites, including Gmail, YouTube, Facebook, Picasa, Google Docs, and Amazon.com. Even search engines could arguably be placed under the SaaS model. Each of these websites offers a service in the form of a relatively simple website where processing is done outside of the user's view. These services behave like

42. *Id.*

a black box: The user inputs information and receives a result, but what happens between the two is hidden.

Two other models, Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), are also described by NIST. They allow users to stack their own software on top of a Cloud platform, giving the user progressively more control over her information.[43] These types of models are not as commonly used by average Internet users, and thus will not be discussed further in this Article.

The NIST definition of Cloud computing is probably the most precise definition that is currently possible, despite its fairly broad scope.[44] This is due to the nature of the Cloud itself. In most basic of terms, the Cloud is the Internet. Almost everything that an average computer user does occurs at least in part in the Cloud.[45] The scope of the impact of this infrastructural shift on privacy, personal information, and copyright is something that one grasps almost intuitively. Let us look at it more closely.

II. COPYRIGHT, CULTURE & THE CLOUD

A. Regulating the Internet

Looking at copyright protection online means asking a very basic question: can governments control the flow of material on the Internet? Peer-to-peer file-sharing has been under relentless legal pressure, to no avail it seems. In some cases, "success" is at hand. In China, Internet control seems to have been far from successful but interestingly based much more on technology to fight technology than on (theoretical) legal remedies.[46] In the first few weeks of 2011, the Egyptian government tried to shut down some or all of the Internet but, given the interconnected and transnational nature of the beast, had limited success.[47] More importantly perhaps, the global outcry was both

43. *Id.*

44. The concept of the Cloud currently occupies a very broad set of functionality. It means different things to companies than to individual users. The NIST definition accounts for that difference by using technical language that accurately reflects the many aspects of the Cloud. *See* Eric Knorr & Galen Gruman, *What Cloud Computing Really Means*, INFOWORLD (Apr. 7, 2008), http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031.

45. Email and browsing the Internet have become two of the most common uses for personal computers. Both of these, by their nature, go into the Cloud to retrieve new email or websites. Social computing websites like Facebook (http://www.facebook.com) or Twitter (http://www.twitter.com) also have a massive amount of users each day, and they use the cloud to store the users' data.

46. *See* Jonathan Zittrain, *The Fourth Quadrant*, 78 FORDHAM L. REV. 2767, 2773-75 (2010).

47. *See* Christopher Williams, *How Egypt Shut Down the Internet*, THE

immediate and extremely loud.[48]

The principal difficulty of regulating the Internet stems from the fact that the Internet was architected using packet switching technology and the ubiquitous Internet Protocol.[49] This makes the Internet independent of the underlying hardware and thus makes it much harder to control than a mainframe-based or hub-and-spoke network with a single brain.[50] In fact, the Internet was precisely that: a shift from a central or mainframe architecture to a client-server architecture in which the Internet basically serves to transport data and allow computers to have an identity (an IP address).[51] The last fifteen years were thus attempts to regulate what amounted "only" to a communication system, a neutral infrastructure to transmit packets of bits from one computer to another. Controlling *that* Internet meant controlling information as it was moving between the computers of individual users.

This raised a number of issues. For example, when trying to enforce copyright in content stored in files on those computers, copyright law had to spar with privacy considerations. Servers stored data, but private data and most data processing functions took place on individual computers in our homes and offices, often within our private sphere, protected by our reasonable expectations of privacy.[52]

Then the attention turned to Web 2.0 and the increasing importance of social networking sites and the use of networks to connect people according to their affinities.[53] Web 2.0 was a sign of things to come. More content stored on Facebook, Flickr, or YouTube's servers and, increasingly, use of all manner of new devices used to connect to and modify that content. Indeed, as noted in the introduction, the Internet has

---

TELEGRAPH (Jan. 28, 2011), http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.

48. *Id.*

49. *See* CARR, *supra* note 9 and accompanying text.

50. *See generally* James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997).

51. This is usually described as the "Transport Layer" and the "Internet Layer." *See* CARR, *supra* note 9, at 54-55; *see generally id.*

52. The Sony Rootkit debacle comes to mind. *See* Lilian Edwards, *Coding Privacy*, 84 CHI.-KENT L. REV. 861, 869 (2010); William Jeremy Robison, *Free At What Cost?: Cloud Computing Privacy Under The Stored Communications Act*, 98 GEO. L.J. 1195, 1233-35 (2010).

53. Gervais noted several years ago in an unpublished piece that this had profound social justice implications, as citizens are no longer confronted with information about all sides of an issue, but rather look for information sources that too often reaffirm preconceived notions and possibly prejudiced views. This makes for a much poorer political and public debate. *See* Daniel Gervais, *Democracy, Technology and Social Justice* (2003) (unpublished manuscript), *available at* http://aix1.uottawa.ca/~dgervais/publications/Gervais%20DemocracyTechnology%20and%20Social%20Justice.pdf.

radically transformed itself. It is no longer a connection among millions of computers on which data is stored and processed. The data—and the software to process it—increasingly resides on the network and thus part of the new network, a communication infrastructure linked to servers with exabytes of content available to all. This scalable and virtual smorgasbord of resources is a by-product of the ease-of-access to remote computing sites, a technology known as Cloud computing.[54]

Access to massive amounts of cultural content in the Cloud and ways to manipulate it may be viewed as a positive development leading to an increase in global cultural—and possibly economic—welfare. It may open cultural access beyond borders and become a great equalizer.

There are more troubling possibilities, however. Governments might like the fact that data and software will reside not on our home computers but on a smaller number of servers.[55] As we note in the fourth part of the Article, there are significant limits to the privacy of content stored in the Cloud, especially after 180 days. In the Cloud, there is a finite number of intermediaries, and those intermediaries are often commercial (though the emergence of a public interest/non-profit part of the Cloud should not be discounted), and they may not have the consumers' privacy as much at heart as individual users themselves. As such, those intermediaries present an easier set of regulatory and particularly enforcement targets.

Access to the Cloud will more often than not be obtained via proprietary devices and private networks that can much more easily regulate the type of traffic they allow. Whether the Internet remains "neutral" is at the heart of this debate.[56] As users increasingly switch to being device-based (from game consoles to cell phones to PDAs, etc.), the open nature of the Internet protocol will be veiled by layers of proprietary code designed to maximize income, not access.

B. The Cloud: The Global Meme Factory

Human culture not only includes songs and stories, but also habits, skills, technologies, scientific theories, bogus medical treatments, financial systems, and organizations.[57] All these bits of human culture tend to be imitated and adapted. As such they are what Dawkins referred to as *memes*, that is, "a unit of imitation."[58]

---

54. *See* Strahilevitz, *supra* note 12 and accompanying text.

55. *See supra* Part I.

56. *See generally* DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE (2009).

57. *See* Susan Blackmore, *The Third Replicator*, N.Y. TIMES OPINIONATOR: BLOG (Aug. 22, 2010, 5:30 PM), http://opinionator.blogs.nytimes.com/2010/08/22/the-third-replicator.

58. RICHARD DAWKINS, THE SELFISH GENE 192 (2d ed. 1989).

The Cloud—once the necessary bandwidth is there to empower it fully—will link all our computers and other digital devices to a virtually infinite array of content and ways to access, process and add to that content, whether as information, entertainment, or both.[59] Naturally, digital availability is a prerequisite to enter the (digital) Cloud. However, the ongoing digitization of large swaths of our pre-digital culture means that most cultural products will be available.[60] This type of generalized access to entire repertories of cultural products is not new, but the Cloud makes it a reality, a *de facto* rule, for almost all cultural production and anyone with Internet access on a mobile phone, computer or other device.[61] There will be more to imitate and more ways to imitate. Hundreds of millions of Internet users are downloading, altering, mixing, uploading, and/or making available audio, video, and text content on personal web pages, social sites, or using peer-to-peer technology to allow others to access content on their computer.[62]

On the positive side of the technology ledger, therefore, Cloud availability means that a new space is open for almost all cultures to access and adapt cultural artifacts from their own sphere and most if not all others. They can speak and share. Indeed, the Cloud is structurally meant to share. Whether one is looking for *Just Before the Battle* by Mother Campbell, the latest Carrie Underwood video, or a picture (and discussion by local experts) of the Hammurabi Code at the National Library of Iraq, it is all there.

And so are, increasingly, your neighbor's summer vacation photos (on Flickr, Picasa or Facebook), your cousin's attempt at playing his new song on YouTube, and a discussion on the best hot dog in Cleveland (we vote for *Old Fashion Hot Dogs* on Lorain Avenue).

Culture is the *store of meanings* that we have available to make sense of our world (meanings embedded in films, music, books, and

---

59. *See* Bernard Golden, *The Skinny Straw: Cloud Computing's Bottleneck and How to Address It*, CIO.COM (Aug. 6, 2009), http://www.cio.com/article/499137/The_Skinny_Straw_Cloud_Computings_Bottleneck_and_How_to_Address_It.

60. The Google Book project is a good example. *See* Pamela Samuelson, *Google Book Search and the Future of Books in Cyberspace*, 94 MINN. L. REV. 1308 (2010).

61. *See* CHARLES LEADBEATER, CLOUD CULTURE: THE FUTURE OF GLOBAL CULTURE RELATIONS 19-23 (2010), *available at* http://www.britishcouncil.org/russia-projects-cultural-creative-economy-useful-resources-cloudculturecharlesleadbeater ("A Bedouin should be connected to the same web of communications as people in Cairo, New York and London. In the space of a decade, mobile phones, Wi-Fi, broadband Internet, satellite and digital television have become commonplace, if not ubiquitous. That has brought in its wake a culture of mass self-expression on a scale never seen before, which has the potential to touch and connect us all and to change how we relate to one another through culture . . . We will also be equipped with more tools to allow us to make our own contribution, to post our photograph or composition.").

62. *See* Gervais, *supra* note 37, at 845-46.

newer formats of cultural dissemination). At no point in history has there been a wider and more open store. This should lead to more global or at least non-geographically bounded memes to emerge.[63] Songwriters and designers have access and are influenced by "foreign" memes in a way that might make "foreignness" itself a very different—and much more relative—notion. Internet blogs and other dematerialized cultural scenes will lead to not only small memes, such as catch-phrases, but also more portentous ones, such as beliefs to emerge and spread. For example, perceived oppression of a cultural group such as Falun Gong is information easily acquired in North America, where it may have lead to a significant increase in Falun Gong membership.[64]

Yet, as any trip to a warehouse-type store will teach us, in a world with fewer familiar or at least traditional landmarks to guide us, the role of *intermediation* in our process to interpret and define our life and our world will increase exponentially. To take a concrete example, in theory the Cloud should make it easier for students, who by now are all born digital, to apprehend their world and fashion a personality reflecting a more global or "ageographic" perspective, if they so wish.[65] The intermediation tools they use may not help them get there. Still, global should be the natural order of things on the Internet—though language and geographical preference software are fighting this infrastructural ability to truly offer the world to us on any device.[66]

Another entry on the positive side of our ledger, Cloud content can be manipulated, mashed up or remixed, and new forms of creation are thus increasingly possible.[67] Then the modified and adapted Cloud content adds to the Cloud, where it also resides, snowballing into billions of new creations.

On the negative side, obviously "available" does not mean free, nor

---

63. *See* JIB FOWLES, ADVERTISING AND POPULAR CULTURE 23 (1996).

64. *See* Claire Wright, *Censoring The Censors In The WTO: Reconciling The Communitarian And Human Rights Theories Of International Law*, 3 J. INT'L MEDIA & ENT. L. 17, 35-36 (2010).

65. Whether current educators and parents, many of whom were not born digital, help develop the desire in their students to go global and celebrate difference rather than fear it is quite a different matter, of course. This will greatly influence whether access to the Global Meme Factory "becomes a protective enclosure for endangered identities rather than something that unfolds and opens out." Charles Leadbeater, *Cloud Culture: The Promise and the Threat*, EDGE (Feb. 2, 2010), http://www.edge.org/3rd_culture/leadbeater10/leadbeater10_index.html.

66. The preference and filters imposed by intermediaries is discussed further *infra* § 2.3. There is, however, another reason to limit our traveling to distant servers. Data costs fractionally more when retrieved from distant locations, but this is usually not reflected in the monthly (flat) subscription rate we pay for online access.

67. *See generally* LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY (2008); HENRY JENKINS, FANS, BLOGGERS, AND GAMERS: EXPLORING PARTICIPATORY CULTURE (2006).

does it mean universal access. Copyright and/or technology can restrict access and/or price to something beyond one's reach, especially if price discrimination is absent. A $10 book download is not quite the same product for the average netizen in Luxembourg and Burkina Faso, because $10 is not the same amount of money in relative terms when the per capita GDP goes from $82,600 to $1,200 (68:1).[68] The absence of price discrimination in developing countries, that is the sale of cultural products at "Western" prices, corrals access to culture to the financial "elite" and adds water to the "culture as elitist" mill.

In an ironic twist in the emergence of a supposedly global Cloud, technology increasingly limits access to a number of cultural products with a higher commercial value based on where the user is physically located.[69] This *should* allow companies to price discriminate and broaden access but, in my anecdotal experience at least, very few actually do.[70]

C. Regulatory Challenges

Regulating any technology that is still inchoate is a hard challenge. Hence, one of the factors that makes Cloud regulation difficult is that the target is moving and may evolve in response to, and resist, attempts to regulate it.[71] As noted above, however, a countervailing force is that the Cloud may in some ways be easier to regulate because access to it, and its operation, require huge investments. Internet Service Providers, server farms, and, more importantly perhaps, companies that will lead us to content, including Google and other search engines, are easier to locate. Regulations would seem easier to enforce than when the targets are hundreds of millions of individual personal computers.

Cloud construction is mostly financed by private investments, and those investors will want to design the Cloud to recoup those investments

---

68. Luxembourg, THE WORLD FACTBOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/lu.html (last visited Nov. 19, 2011); Burkina Faso, THE WORLD FACTBOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/uv.html (visited Nov. 19, 2011). The Berne Convention for the Protection of Literary and Artistic Works (Sept. 9, 1886, S. Treaty Doc. No. 99-27, 331 U.N.T.S. 218) is the main copyright treaty with 164 member countries (as of January 2011—*see* www.wipo.int) has reflected this need for differential treatment since the addition in 1971 of an Appendix allowing developing countries to reproduce and translate books to make them available at a lower price.

69. For example, NetFlix is unavailable outside the US and Canada. *See* NETFLIX, www.netflix.com (last visited Nov. 19, 2011).

70. This seems a sad yet highly intuitive market reality. Building a pricing system that can efficiently price discriminate will cost more, and likely target lower capacity markets. Why would Amazon want to spend money to develop the ability to sell $1 Kindle download to readers in poorer countries? If this is true it would support the need for non-commercial digital libraries, perhaps with government support, at least in the form of regulation. *See* LEADBEATER, *supra* note 61, at 15-16.

71. *See* Daniel Gervais, *The Regulation of Inchoate Technology*, 47 HOUS. L. REV. 665 (2010).

and generate appropriate returns for their shareholders.[72] From this perspective, the major public-interest regulatory challenge linked to the growth of the Cloud will likely be reconciling commercial interest and free markets with the fact that a small number of major companies will be the guardians of the Cloud, which in turn is the repository of our digital culture. Companies, not governments, will control our day-to-day interaction with the Cloud.

Because one might fear the emergence of *de facto* monopolistic tendencies—even though not all monopolies are abused—governments might want to intervene from a competition policy perspective to ensure that there are several "Clouds." There will be, as one can plainly see, a major tension between two regulatory reflexes, however: (a) supporting a reduction in the number of control points on the Internet (a few Guardians of the Cloud as easier targets); and (b) ensuring a sufficient degree of competition (i.e., multiple Clouds). The enormous importance gained by intelligence and national security-related controls of the Internet since 9/11 would seem to support the former (fewer and larger players).[73] In large part it will be up to civil society and non-profit entities to ensure that the second objective (competition and a reasonable degree of openness and access) remains present in the minds of policymakers. The desired result might take the form of public Clouds, with commercial Clouds developing in parallel.

The risks are real and some observers are already close to a call to digital arms. Referring to the proposed Google Book Settlement as a precursor of a future Google-dominated Cloud, Charles Leadbeater noted that "this possibility, a vastly enhanced global space for cultural expression, is threatened by intransigent vested interests, hungry new monopolists and governments intent on reasserting control over the unruly web. "Judge Chin's court is a microcosm for the arguments that will rage over the control of culture globally in the decades to come."[74] At this juncture, the potential abuses that might arise if the Cloud is left entirely unchecked have yet to materialize on a scale that would warrant massive intervention. Additionally, the nature of the optimal remedies may not be easily determined. If, for instance, one were to decide that Google is abusing its *de facto* monopoly on digitized books, would compulsory access be the best solution? Or should public libraries digitize their own books? While the former seems easier, the optimality

72. The paradigmatic nature of the shift is best illustrated by the fact that access to a book (other than by purchasing a copy) will no longer be provided by a public library; it will be provided by Google Books.

73. *See* Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 139-152 (2010).

74. *See* LEADBEATER, *supra* note 61, at 16.

of remedies may reside in the latter. For example, public librarians around the world may be far better equipped to determine which books or other content to make available from their own culture. Librarians—non-judicial public resources—might greatly improve not just access, but the quality of the Cloud in ways that a "Cloud capitalist" and judges might not. Still, to defeat its critics Google would have to perform to a probably impossibly high degree of global corporate citizenship and show unparalleled cultural sensitivity.

The most significant risk we see is defective or suboptimal intermediation in Cloud access and content generation. Because *everything* is or will be available in the Cloud, technology will necessarily be used to locate and manipulate content. Some of it seems benign, like a Google search results page, but even that implies a neutrality and efficiency of the results. Google already uses AdWords to complement "natural" search results. Should neutrality (or the "naturalness") of search results be regulated? If so, how? Some might suggest that having multiple intermediaries might be a better option, trusting competition to lead users to intermediaries offering better results.[75]

Several technologies used to manage our relations with the Cloud are not quite as benign as search engines. In fact, some are inherently problematic. First, as Amazon and Google users know all too well, *the Cloud knows you*. And the more one uploads to and interfaces with the Cloud, the more it knows you. Facebook and LinkedIn suggest "friends" and contacts. Is this is a problem or a positive development? Clearly, the major users of this knowledge are providers of targeted advertising. Whether getting more targeted ads is a benefit for consumers is debatable. One can see the advantage of being informed of the availability of a new product. By the same token, this may lead to overspending. This is mostly beside the point, however. The real concern is that when those technologies suggest content, they may interrupt a chain of events (initiated by a user's search) that might have led one to a completely different place. They reinforce the past but at the potential expense of different futures. When Amazon suggests a book for instance, one may end up buying that book and not wander in a different cultural "direction." Then again, it may be that those suggestions will incrementally broaden a consumer's cultural geography. Whether this is a positive development overall should be tested empirically. However, because "Cloud suggestions" (and default choices made for users) are based on one's past actions and preferences, intuitively they will tend to reinforce what one already knows and who that person is rather than

75. *See* Samuelson, *supra* note 60.

allow one to take a different path. In other words, they might expose each of us to "more of the same." The risk is that this may, in time, impoverish the social and cultural discourse.[76] The undeniable fact remains, however, that when every bit of culture and digital content is in the Cloud, the key will be to locate and access content that one is interested in. In McLuhanesque terms, intermediation is the new content, and intermediates the guardians of the Cloud.

The commercial paradigm of the Cloud (that lawmakers and many others, including the music industry still do not get) is not one of scarcity of supply. It is, in fact, exactly the opposite.[77] What is happening is a shift similar to the shift from mechanical to quantum physics. Let us call it "quantum market economics" for the "content industries." The first law of the new environment is that *the value of an information object on the Internet is not derived from its scarcity but rather from the fact that those who value it most will find it.* The preference-dictating algorithms mentioned above are based on a user's past. They assume that a user will value what she valued in the past and keep her in your "value zone." However, serendipitous Cloud wanderings—a la Thoreau in his woods—might have led her to value cultural products she did not know. The Cloud, like a park ranger, wants you to stay on the marked path, where it knows you.

This is not necessarily bad. In a world where everything is in the Cloud, the inescapable truth is that the value of a particular cultural artifact is an amalgamation derived from the number of users connected with that content they themselves value individually. Network effects create huge value. And the individual connections that lead to the emergence of Cloud value are established by the intermediaries. Whether they are benign and "natural" in establishing those connections or whether they will guide you according to (completely understandable) revenue-maximizing goals, intermediaries will become the true

---

76. *See* Gervais, *supra* note 53.

77. *See* Daniel J. Gervais, *The Role of Copyright Collectives in Web 2.0 Music Markets*, *in* THE SELECTED WORKS OF DANIEL J. GERVAIS 1, 1–2 (2007), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1010&context=daniel_gervais ("While opinions and studies—both the data they use and their analysis—are open to disagreement, the fact remains that the laws of physics that applied to the sale of physical copies of records, CDs and the like do not seem to apply to the Internet, which seems counterintuitive to market experts trying to apply traditional rules such as scarcity of supply. There is no scarcity of supply here. Nor are traditional laws of pricing of physical goods directly applicable because the market for authorized music is competing with 'free.' What is needed, then, is a shift similar to the shift to 'quantum physics.' Let us call it 'quantum market economics' for the music industry. The first law of this new environment, as I have argued in a number of past publications, is that value of an information object on the Internet is not derived from its scarcity but rather from the fact that those who value it most will find it. This explains the tremendous value of companies like Google, at least as far as its traditional role as 'finder' of information objects is concerned.").

Guardians of the Cloud, the Global Meme Factory, and our culture.

There are other challenges ahead. Let us take a less US-centric perspective. In the United States, while we may accept a certain degree of governmental control and monitoring subject to court supervision, we tend to assume freedom of speech is a key value in the policy equation of Cloud control. That is gravely mistaken. The Cloud is at risk of control by authoritarian governments. The Internet, whether structured as a pure communications network or designed as a Cloud, is intensely political. In fact, in the words of Evgeny Morozov, "information also becomes the most politicized of global commodities."[78] China's attempts to control the Cloud are well documented.[79] In Russia, social networking sites are used to criticize political leaders.[80] And Egypt and other Arab countries recently tried to gain control of what could be transmitted. The list is long and will get longer. Has the Cloud added resilience to information? While information stored on a personal computer is at risk and evanescent, once firmly rooted in the Cloud, information is much harder to delete. Law may seem powerless, but technology that prevents access might achieve a similar result. If the Cloud does prove easier to control than the current Internet, we will have taken an important step backwards for freedom of speech.

But for the average Cloud user, the most direct form of regulation might well be intellectual property and copyright *primus inter pares*.

D. Copyright & The Cloud

Copyright emerged as a policy lever to organize the market for books. Its first modern incarnation is probably the Statute of Anne of 1710.[81] The explanation is simple enough: If a publisher can just sit and wait to see which new books do well and then copy them, the incentive to invest in production of new books is diminished and cultural output may suffer.[82] A similar reasoning applies to music and to several other products. A film studio might want to decide through which medium a film is to be released and when.[83] The paradigm of this type of cultural

78. Evgeny Morozov, *The 20th Century Roots of 21st Century Statecraft*, FOREIGN POLICY (Sep. 7, 2010), http://neteffect.foreignpolicy.com/posts/2010/09/07/the_20th_century_roots_of_the_21st_century_statecraft.

79. *See* Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering Worldwide*, BERKMAN CENTER FOR INTERNET & SOCIETY, http://cyber.law.harvard.edu/filtering (last visited Nov. 19, 2011).

80. NIK GOWING, SKYFUL OF LIES AND BLACK SWANS: THE NEW TYRANNY OF SHIFTING INFORMATION POWER IN CRISIS (2009).

81. *See* MARK ROSE, AUTHORS AND OWNERS: THE INVENTION OF COPYRIGHT 36 (1993).

82. *See* Samuelson, *supra* note 60.

83. *See* BRUCE M. OWEN & STEVEN S. WILDMAN, VIDEO ECONOMICS 29-30 (1992).

commerce is the well-documented phenomenon of scarcity: New products are relatively scarce and must be obtained from an authorized source.[84]

It seems self-evident (at least to observers not part of the entertainment industry) that the Cloud is not the commercial equivalent of selling physical goods. Yet, laws are called upon to maintain the scarcity paradigm. Let us consider why this makes little sense. In a store, one browses a finite selection. The store typically sells a limited number of categories of goods. There is usually signage to help the consumer make her selection. Advertising and product placement may be used to "guide her hand."

Some of this is replicated online, of course.[85] However, the impact is different, and so should the metrics be. Aggregate (commercial) value on the Internet, as I noted in the previous section, is derived from connecting people with content they value individually. An MP3 downloaded on a computer may be counted as a form of piracy worth $2, but the reality is that *the user assigns the value*. She may have downloaded a song "just because" and never listened to it. Perhaps it was recommended by a friend, downloaded, listened to once and then quickly forgotten. This music has little or no Cloud value if all users treat it that way and if those who might like it are not connected to it. Conversely, if the Cloud can connect a user with a song (and/or an artist)—whether from down the street or the other side of the planet—value flows to both the content provider and the user as that user becomes a fan and value-generator. She may buy music, tickets, merchandise, and ultimately become a social site spokesperson for the artist. Then, and only then, does the music have "Cloud value."

E. International Intellectual Property Rules

The main set of international intellectual property rules are contained in the TRIPS Agreement.[86] The Agreement was part of a package of trade rules signed at Marrakesh in April of 1994. It entered into force on January 1, 1995.[87] It was negotiated between 1986 and 1994, though mostly completed by the end of 1991.[88] The World Wide

84. *See* Claus Thustrup Hansen & Søren Kyhl, *Pay-Per-View Broadcasting of Outstanding Events: Consequences of a Ban*, 19 INT'L J. INDUS. ORG. 589, 601-04 (2001).

85. Online advertising is at least as prevalent as it is in other media.

86. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, *available at* http://www.wto.org/english/docs_e/legal_e/27-trips.pdf [hereinafter TRIPS Agreement].

87. Overview: The TRIPS Agreement, WORLD TRADE ORGANIZATION [WTO], http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (last updated 2011).

88. *See generally* DANIEL GERVAIS, THE TRIPS AGREEMENT: DRAFTING HISTORY AND

Web emerged in the public sphere in 1993 with the release of the Mosaic browser.[89] It was not until a few years later—some might say not until the Napster lawsuits—that the size of its potential impact on the market for copyrighted goods became fully visible.[90] It is not surprising, then, that TRIPS is not expressly equipped to deal with the Internet.

The World Intellectual Property Organization (WIPO) tried to fill the gap in December 1996 with the adoption of its two "Internet" treaties.[91] The treaties provide a right of making available, but also, and more importantly it seems, a right to prevent the circumvention of technological protection measures (TPMs) used to restrict use of copyrighted content.[92] In the United States, the treaties were implemented by the Digital Millennium Copyright Act (DMCA).[93]

Part of the negotiated DMCA package was that Internet Service Providers and search engines would not have liability for letting users access infringing material.[94] The regulatory effort here has a clear direction: limit access and use. In other words, the aim was to reinstate the scarcity paradigm for industries that still count "units" sold.[95]

There is little doubt that the best way to maximize value on the Internet is *not* to control individual uses. But old habits indeed die hard, and this one (control) may not die—at least not until the industry itself is gone. A number of important stakeholders, including songwriters, seem to agree.[96] The optimal solution self-evidently would leverage network

---

ANALYSIS 11-27 (3d ed. 2008).

89. *See* J.R. OKIN, THE INTERNET REVOLUTION: THE NOT-FOR-DUMMIES GUIDE TO THE HISTORY, TECHNOLOGY, AND USE OF THE INTERNET 110 (2005).

90. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

91. WIPO Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17 (1997), 36 I.L.M. 65 (1997) [hereinafter WCT], *available at* http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html; WIPO Performances and Phonograms Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17 (1997), 36 I.L.M. 76 (1997) [hereinafter WPPT], *available at* http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html.

92. WCT, arts. 8 and 11; WPPT arts. 10, 14 and 18.

93. Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-05 (2004). On the intent, *see* S. Rep. No. 105-190, at 2 (1998).

94. *See* JESSICA LITMAN, DIGITAL COPYRIGHT 127-45 (2d ed. 2006). Services hosting content that a copyright holder considers infringing would, however, have to set up a contact point for notices sent by the copyright holder to take down such content. *See* 17 U.S.C. §§ 1201-05.

95. The *Recording Industry in Numbers 2010* report published by the International Federation of the Phonographic Industry [hereinafter IFPI] still considers units sold as a key statistical component of the report. For example, the page on Belgium shows a decline from 2005 to 2009 from 14 to 10.7 million CD "units." *See* IFPI, RECORDING INDUS. IN NOS. 2010 31 (2010), *available at* http://www.ifpi.org/content/library/RIN-samplepage-2010.pdf.

96. *See The Songwriters Ass'n of Canada's Proposal to Monetize the Non-commercial Sharing of Music*, SONGWRITERS ASSOCIATION OF CANADA, http://www.songwriters.ca/proposaldetailed.aspx (last visited Nov. 19, 2011). In parallel, one of the four remaining labels, EMI, was taken over by a creditor. *See* Dana Cimilluca & Ethan Smith, *Citigroup Takes Control of EMI*, WALL ST. J., Feb. 2, 2011, at B6, *available at*

effects and maximize value by maximizing connections between content and those who value it, which includes allowing no-value or little value connections to be established probably as a multiple of the connections that do bring value. In very concrete terms, it may be that ten people will download a file for one who will truly appreciate it. But to find that one, it is often necessary to allow the ten. This is hardly reconcilable with copy-control models trying to replicate physical scarcity of supply online.

Yet many sectors of the entertainment industry still aim to convince policy makers to stamp out "piracy," which seemingly includes every unauthorized access or download of copyrighted content. Unfortunately, a lot of this piracy is without actual value to anyone. It is also piracy based on the current model of downloads and storage on one's computer.[97] This may disappear both because devices may have less storage—this is in all likelihood an epiphenomenon—and because the Cloud is designed to provide constant access to "everything," in a world that is always online, thus avoiding the need for local copies. We are not there yet, and "Internet everywhere" is far from being a reality. But access is also possible using cell phones and other proprietary networks. As we move away from an open architecture based on the Internet Protocol to more proprietary access and access on demand as a rule, it will become easier for the entertainment industry to live its ultimate dream—complete "fared use."[98] A dream in which each use is ultimately linked to a micro-payment or possibly part of a contractually and technologically cabined subscription-based pricing model.

Ironically, the repeated suggestions to license file-sharing in an environment that the music industry could have set up and loosely controlled, but which it has continuously scorned by the recording industry, will likely be the outcome. But it will come with control wrestled away from the content provider and into the hands of the Cloud's real guardians, the intermediaries. Google Music is coming.[99]

An open question is whether users—especially those under-30 most of whom have learned to access music and a number of other cultural products via peer-to-peer networks *first*—will easily abandon the "try to

---

http://online.wsj.com/article/SB10001424052748703445904576118083710352572.html.

97. A basic computer now sells with somewhere between 500 GB and 1 TB of storage. Even in CD quality format, this allows for the storage of tens of thousands of songs.

98. *See* Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998).

99.Actually it started as an experiment in China, but in a market with basically no authorized market and still requiring behavior modifications. Not surprisingly, it was not a huge success. *See* David Barboza & Brad Stone, *China, Where U.S. Internet Companies Often Fail*, N.Y. TIMES, Jan. 15, 2010, at B1, *available at* http://www.nytimes.com/2010/01/16/technology/16failure.html.

see if you like" model and willingly jump onto an obsolete bandwagon; namely, a world in which what matters is not how many people enjoy a particular song or artist but how many copies of a file are in existence at any point in time. They may not, and oddly enough personal computers and other IP-based (i.e., non-proprietary) devices may be used more because they can defeat a pure fared use world. By the same token, device manufacturers might respond to that demand and provide devices that do not force users to take steps to continue to enjoy cultural products the way they want.

There is now an effort afoot to multilateralize the DMCA, increase penalties, and generally add layers of enforcement access and use controls. "Newspaper taxis . . . Waiting to take you away," as the Beatles might say.[100] But, the song continues, "[c]limb in the back with your head in the clouds, [a]nd you're gone."[101] This is an apt metaphor. The old copyright paradigm is perhaps best epitomized by fast-disappearing newspapers.[102] But climb in the Cloud, and you're gone. Gone into a different access paradigm, one in which trying to connect to what matters is what matters.

These efforts apparently include an attempt to rewrite the rulebook on ISP and search engine safe harbors. This attempt, the Anti-Counterfeiting Trade Agreement (ACTA), is the application of Statute of Anne scarcity to a 21st century Cloud where a copyright holder should seek to maximize access (and the number of people who pay, in one form or another) for such access, and not to minimize the number of "units" accessed without payment, because that is not how value is derived.

The futility of this attempt (so far) as an empirical matter is compounded by the fact that access restrictions tend to reduce commercial value in the Cloud. The music industry's attempt to funnel every music lover to a single, TPM-restricted download is clearly not optimal. In fact, any major behavior change such as dropping peer-to-peer clients for systems imposing controls overuse and offering a more limited repertory have not done well. The industry's bottomline is exhibit 1.[103]

The Cloud is a repository of content and users will want access to that content whenever and on whatever device they happen to have at

100. THE BEATLES, *Lucy in the Sky with Diamonds*, *on* SGT. PEPPER'S LONELY HEARTS CLUB BAND (Capitol Records 1990) (1967), *available at* http://www.sing365.com/music/lyric.nsf/lucy-in-the-sky-with-diamonds-lyrics-thebeatles/268f467b6ecc8c7148256bc20013fdb3.

101. *Id.*

102. I am still amazed that based on our anecdotal data, law students think of the "New York Times" mostly as a web site and source of information, not as physical thing (paper).

103. *See* IFPI, IFPI DIGITAL MUSIC REP. 2011 (2011), *available at* http://ifpi.org/content/library/DMR2011.pdf.

that point in time, not units to store. They will want to experience as many of the cultural products they value as possible, and they likely will value intermediaries who lead them to more (in spite of the limiting effects that this may have as discussed earlier). Cultural industries that will do well in the Cloud will be Sherpas, not park rangers.

Intellectual property rules make this possible, but the solution is licensing and more access, and enforcement limited to professional pirates.

Recent efforts such as the Anti-Counterfeiting Trade Agreement (ACTA), are not necessarily negatives; it all depends on how they are used and implemented.[104] ACTA may be, however, a poster child for a view of how the Cloud should develop, tailored to a desire to control access to cultural products as "controlled units," instead of acknowledging that the Cloud is amorphous and ultimately, everywhere. Control makes little sense, at least if the aim is to maximize income. The Cloud is a formidable distribution vector. Value will not be derived from counting (or limiting units) but by connecting people, wherever they may be, to content they value. Each connection adds value.[105] Deleting or limiting copies (i.e., replicating scarcity of supply) in such an environment seems an anachronism at best. Yet it arguably informs current attempts to beef up enforcement against individuals and, more tellingly, intermediaries.

At this critical juncture, it would be unfortunate if a major policy development effort were to be based on a misguided strategy with erroneous assumptions about what motivates consumer behavior. Policy makers cannot be rainmakers in the age of the Cloud. ACTA cannot be an alternative to a real discussion on optimal access to cultural products and ultimately a stand-in for new thinking on business models.

III. PRIVACY

A. Personal Information in the Cloud

Think about the last time you sent an email from your web mail account to a friend or family member, or the last time you logged onto a banking website to check your account balance, or even the last time you

104. On ACTA, *see* ACTA Fact Sheet, OFFICE OF THE U.S. TRADE REPRESENTATIVE (Mar. 2010), http://www.ustr.gov/acta-fact-sheet-march-2010 (last visited Nov. 19, 2011).

105. The so-called network effects. Those effects are "a characteristic of a product by which its value to the consumer is defined or enhanced by virtue of other consumers adopting the same product. The identifying characteristic of a product with network effects is its ability to connect one consumer, or "user," to other users of the same product." John McGaraghan, *A Modern Analytical Framework For Monopolization In Innovative Markets For Products With Network Effects*, 30 HASTINGS COMM. & ENT. L.J. 179, 189 (2007).

shared the family pictures you just took online so your family could download them. All of these tasks that have become so mundane to so many people take advantage of the power of Cloud computing to connect you to the people and sites you requested. But what happens to the information when it disappears into the Cloud? Where are your passwords and your account numbers saved? Who can access them and what do they do with them? Can you delete the information, in the sense that no one will be able to access it in the future?

Cloud computing has become such a vital part of many peoples' lives and information about people has become a commodity in its own right. Companies commanding vast portfolios of data about Internet users that account for large chunks of their worth, are using information in the Cloud to advertise and market in an increasingly focused way.

In its earliest description by Justices Warren and Brandeis, privacy was described as a "right to be let alone."[106] If one did not share a bit of information, it was private. If one did tell someone, then that information basically became public. This simple binary analysis is not wrong and probably fit quite well into the society of the day. Cameras and telephones were relatively new advancements, and the main method of recording or sending any sort of information was by handwritten letter or telegraph. It is easy to argue that that a letter contained in a sealed envelope and sent to a certain individual is of a private nature and should not be read by others without permission. The Justices could not have guessed to what degree the transportation of information would change over the intervening century, or the extent to which information is stored, used, and manipulated.

The dramatic increase in the complexity of the communications systems between then and now has led to a corresponding increase in the level of difficulty in ascribing a specific meaning to the notion of privacy. At the very least, the binary approach is now a range of possibilities; black and white has been replaced by shades of gray. With the advent of the Cloud and the associated culture of accessing everything from shared, anonymous servers, privacy is no longer a matter of keeping information private. The servers are not private; they are operated by providers of Cloud services. Information is thus "disclosed" to the Cloud. What happens on the Cloud is a matter of contract law, of course, but also of the application of statutory mechanisms to servers which cannot claim private status, unlike a PC in one's home or a device in one's pocket. The Cloud necessarily implies relinquishing some degree of privacy protection.

As a technical matter, providers of Cloud services can probably

106. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

access any material uploaded to the Cloud. As a legal matter, privacy is about control over who gets access to what information. Put differently, privacy is about controlling what is done with information after it is released to the Cloud. "When we complain about infringements of privacy, what we really demand is some measure of control over our reputation in the world. Who should have the power to collect, cross-reference, publicize, or share information about us, regardless of what that information might be?"[107]

As it currently stands, many providers of Cloud services obtain a license (which users accept by clicking but perhaps also without reading) to use the personal information uploaded to the Cloud in exchange for access to free services. These services typically support their business through advertising. They use personal information to target ads, ensuring the maximum amount of business for advertisers. We are not suggesting that there is something inherently wrong with this system, assuming that the companies are properly licensed to use the consumers' personal information in that manner. In fact, for many consumers, this may be a good deal. We are suggesting, however, that the permanency of the information uploaded to the Cloud and the unforeseen ways in which it may be used do constitute a significant potential downside.

Basically, the problem is that the consumers are relinquishing control of their personal information, and of their online identity, to these companies. They may thus lose the ability to define their appearance to others on the Internet and the related ability to maintain and define their individuality. That may seem extreme given the pervasiveness and success of Cloud services, but it is important to remember how valuable the vast quantities of information that advertisers, employers, and other entities have access to, and how easy it is to abuse that information. Once personal data is in the Cloud, there is no way to know with certainty where it is stored, which laws apply to that storage, and who might see it. In certain cases, it may simply not be possible to truly delete the information.[108]

The fact that average users do not know how personal information is used after it enters the Cloud demonstrates clearly the outdated nature

---

107. Siva Vaidhyanathan, *Naked in the 'Nonopticon'*, CHRON. HIGHER EDUC., Feb. 15, 2008, at B7, *available at* http://chronicle.com/article/Naked-in-the-Nonopticon/6197.

108. Due to the nature of the Internet, it is almost trivially easy for others to save and hold onto any information that appears on the Internet publically. Every time a website is accessed, that person is downloading the website onto their own computer (usually into a "cache"). This means that the moment a piece of information goes public, the owner instantly loses the ability to ensure the complete deletion of the information. There is even a site (The Wayback Machine at www.archive.org) that archives websites from the past, allowing users to browse through billions of websites that may have been taken down/destroyed over a decade ago by the owners.

of the dichotomous theory of privacy previously discussed. Of course, a Cloud service user often releases personal information knowing that it will be considered more or less public.[109] An argument can be made that the risks of disclosure were known and assumed. However, this is not an ideal result for the user because having a presence in the Cloud (such as a Facebook page) is important for many users and probably unavoidable for some, and as such the "choice" appears rather theoretical. Yet annihilating the protection of users' data could have a chilling effect on the use and development of the Cloud. This is a two-way-street and both sides are pulling towards greater release of personal information. There is demand for personal information from users of social sites, and providers of Cloud services want more of that information to target their advertising and other services. At the level of the trees, it seems no one has a strong interest in protecting privacy. At the level of the forest, however, the longer term impact of jettisoning large swaths of protection of personal information online means that that protection is basically abandoned because "online" is increasingly synonymous with "everything."

There are a few unavoidable Cloud providers such as Facebook and major email and instant messaging providers. Their services have become so pervasive and heavily used that their position in the bargain for information completely overpowers the individual user. With hundreds of millions of users apparently unconcerned about the protection of their personal information, giants like Google and Facebook have no real reason to support policies that give users control over their information. Users concerned about their personal information are left with no good answer. Either they don't use the service and risk being left out in the cold, or they use the service and trust the provider not to use their information in some undesirable way. As a matter of contract law, the differential in bargaining power arguably affects the validity of major waivers of protection in license and other end-user agreements.

For users who decide to trust the provider, what happens when a user wishes to quit? Upon doing so, it is up to the user once again to trust that the provider will delete her information. The opposite may be true in other cases (bank, online brokerage). Here the user may wish that the provider retain the information (e.g. for a possible tax audit). Though this is anecdotal and would require empirical verification, we have not seen clear obligations undertaken by providers of services such as online

109. While the data may be difficult to gather, it would be useful and interesting to find out empirically what percentage of Cloud service users actually read the privacy agreements and understand the extent to which their personal data is being used by service providers. This study would likely find that the majority of people have a limited understanding.

email and messaging, or brokerage services either, to completely delete or conversely retain personal information for a specific period of time after the user quits. This may constitute a normatively undesirable incentive for users to not change providers and thus retrain competition.

Another example of the use of personal information by a service provider is in search algorithms. As in the targeted advertising context, a number of search engines gather information about a user based on previous searches and other information they may have on that user, such as location and age. The search engine uses that information to display results that the person is more likely to consider a match. This practice and the resulting efficiency gains seem desirable for the most part. However, it is fairly easy for search engines to abuse this power.

Due to the complexity of the Cloud infrastructure, privacy cannot be treated as a private/public dichotomy. Privacy is measured on a spectrum of information accessibility. We suggest that users, that is, us, should have ultimate control over as much of that information and its access and storage as possible. Users should have access to methods of obtaining knowledge about the existence and use of personal information as well as recourse for potential abuses. Current U.S. law provides very few of those safeguards.

IV. PROTECTING PERSONAL INFORMATION IN THE CLOUD

A. Using Currently Available Means

The Fourth Amendment protects people and their property "against unreasonable search and seizures."[110] This includes a number of rights first recognized by the Supreme Court in *Griswold v. Connecticut*.[111] The opinion of the court in *Griswold* described the existence of the penumbral right to privacy:

> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance . . . . Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' The Fifth Amendment in its Self-Incrimination Clause enables the citizen

110. U.S. CONST. amend. IV.
111. Griswold v. Connecticut, 381 U.S. 479 (1965).

> to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.'[112]

While this penumbral right is used to defend privacy and protect personal information, the Constitution is only controlling for situations where the *government* wants to infringe on the individual's privacy. It does not directly govern conflicts between two private parties. Due to this limitation, the protection of the privacy of individuals had to develop down other avenues, including both statutes and case law.

Fourth Amendment jurisprudence applied to a technology allowing the capture and storage of personal information probably began with *Katz v. United States*.[113] Contrary to the 1928 case *Olmstead v. United States*, *Katz* held that wiretapping (access but also possible taping) a phone conversation without the consent of the participants constituted a search.[114] *Katz* was extremely important as a first step toward the proper treatment of electronic communication as a form of private conversation. Notably, *Katz* is also the first case in which the phrase "reasonable expectation of privacy" is used, which appears in a concurrence by Justice Harlan.[115] This phrase would become an important test used for determining whether a communication should be considered private or not, and it is still affecting privacy jurisprudence today.

The Supreme Court was not alone, however, in attempting to protect the privacy rights of citizens. Congress adopted a number of statutes in order to secure private communications against intrusion. The most recent is the Electronic Communications Privacy Act of 1986 (ECPA).[116] This Act is arguably the most important statute protecting the privacy of personal information on the Internet. The goal of the statute is to protect what it deems to be electronic communications from unwanted interception by both state and private actors. Due in large part to the complexity of the issues, difficult questions about the exact scope of the statute have been decided by the courts. Most of these cases dealt with government interception of communications for the purposes of criminal prosecution, rather than privacy issues between private parties. However, many of the holdings illustrate the scope of protection that the ECPA provides.

The law has three different parts. Title I of the ECPA (Wiretap Act)

---

112. *Id.* at 484.

113. Katz v. United States, 389 U.S. 347 (1967).

114. *See generally id.*; Olmstead v. United States, 277 U.S. 438 (1928).

115. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

116. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22 (2006); 18 U.S.C. §§ 2701-12 (2006); 18 U.S.C. §§ 3121-27 (2006).

protects communications in transit.[117] Title II (Stored Communications Act) protects the storage of electronic information.[118] Title III (Pen Register and Trap and Trace Statute) protects dialing, routing, or addressing information that is not part of the communications but can reveal which parties are communicating.[119] We will focus on the first two titles because they are directly involved in the protection of personal information against unauthorized access and storage.

The Wiretap Act protects against both government and private intrusion into electronic communications. The protection is strong in most situations. Access requires a search warrant and any evidence obtained in violation of this part of the Act is subject to exclusion in court proceedings. While the Act provides a powerful tool for protecting privacy, there is a significant degree of confusion concerning its application to communications through the Cloud. Additionally, the statute essentially protects citizens against the use of their personal information in court if illegally obtained and against access to this information by wiretapping, but it does not protect more generally against access to such information or its use in different contexts.

In trying to decide how the statute might apply to the Cloud, we can start with *United States v. Ropp*.[120] The defendant was charged with an interception under the Wiretap Act. The defendant had placed a device that intercepted signals from a person's keyboard to their computer. The question was whether the information that was being typed was covered under the Wiretap Act. The question before the court was whether a message that was being prepared (typed) but had not been sent could be considered "in transmission."[121] The court decided that the signals were internal to the computer and not being transmitted "by a system that affects interstate or foreign commerce" as defined in the Wiretap Act.[122] This holding reflects a key limitation in the coverage of the Act. The opinion of the court mentions that the defendant was clearly "engaged in a gross invasion of privacy" by his actions, but the court could find no hook in the statute to hang his actions on.[123]

Similarly, in *United States v. Scarfo*, the court determined that keystroke signals were not an electronic communication transmitted under the Wiretap Act.[124] In that case, the FBI had installed a keystroke logger which only logged keystrokes when it detected that the computer

117. *Id.*
118. *Id.*
119. *Id.*
120. United States v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004).
121. *Id.* at 835.
122. *Id.* at 837.
123. *Id.* at 838.
124. United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

was not accessing a network.[125] This was a transparent effort to ensure that the rules of transmission under the Wiretap Act would not apply to the act of tapping the computer.[126]

By contrast, in *United States v. Councilman*, the defendant was intercepting emails that transited on a server he controlled.[127] The defendant argued that the emails were being stored, not transmitted, when he intercepted them, so the Wiretap Act did not apply to his actions.[128] The court disagreed and said that the emails were protected while in storage because storage was incident to a transmission.[129]

O'Brien v. O'Brien is another case that tests the limits of what can be considered a transmission.[130] In that case, a Florida state statute that was essentially the same as the federal Wiretap Act was treated in the same manner.[131] Mrs. O'Brien had installed software to monitor her husband's instant messaging and which stored the messages so that she could read them at a later date.[132] The court had to decide whether the messages were being intercepted or just being observed after they had gone into storage on the computer.[133] The wife argued the latter, but the court found against her, finding that her actions had violated the Wiretap Act.[134] While the messages were being transmitted virtually instantly, the fact that the software was copying the messages contemporaneously with the transmission meant that they were being intercepted in violation of state law, which was similar to the Wiretap Act.[135]

Finally, in *United States v. Jones* the court held that text messages held in storage were electronic communications not protected under the Wiretap Act because they were no longer in transmission.[136] This case helps to show where the Wiretap Act stops and where the Stored Communication Act begins. This line is important because the Stored Communications Act does not offer the same protection as the Wiretap Act.

As noted already, the Stored Communications Act (SCA) is the second part of the ECPA.[137] The coverage of this Act is slightly wider in scope than the Wiretap Act, as it potentially protects almost any sort of

125. *Id.* at 574.
126. *Id.* at 582.
127. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).
128. *Id.* at 71.
129. *Id.* at 79.
130. O'Brien v. O'Brien, 899 So.2d 1133 (Fla. Dist. Ct. App. 2005).
131. *Id.* at 1134.
132. *Id.*
133. *Id.*
134. *Id.* at 1137.
135. *Id.*
136. United States v. Jones, 451 F. Supp. 2d 71, 90 (D.D.C. 2006).
137. Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2006).

electronic communication that is in storage. This covers nearly all information in the Cloud that is no longer in transit from sender to recipient. This large coverage is tempered by much weaker protection than is generally provided by the Wiretap Act. Under the SCA, stored communications lack some of the warrant protection that in-transit communications enjoy. The statute does provide for a criminal punishment in the case of unauthorized access of communications stored by certain types of facilities.[138] The statute describes two different types of facilities with different rules for the purposes of the government gaining access to stored data in those facilities. An "electronic communications service," or ECS, is defined as ". . .any service which provides to users thereof the ability to send or receive wire or electronic communications."[139] A "remote computing service," or RCS, is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[140] The difference between these two types of systems reflects the law's desire to lower privacy protection for communications away from the moment of transmission. The ECS is the service that grants the user the ability to send the messages. It is the RCS that is responsible for storing or processing by using an ECS. Not surprisingly, the protection of RCS stored communications is weaker. Communication stored by an ECS is protected for up to 180 days by warrant requirement against government intrusion, while communication stored within an RCS only requires a subpoena or court order with prior notice to the user or a warrant with no prior notice to the user for the government to obtain access.[141]

In *Quon v. Arch Wireless*, the Court had to draw a distinction between ECS and RCS.[142] A police officer was using his work pager to have personal conversations, and the wireless carrier had released transcripts of the messages to the city.[143] If the company was an RCS, then they were within their rights to release the transcript, but if they were an ECS, they violated the SCA by releasing the messages to someone who was not one of the parties to the messages without a

138. *See id.* § 2701(b).

139. *Id.* § 2510.

140. *Id.* § 2711.

141. *Id.* § 2703.

142. Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), *rev'd and rem'd sub. nom.*, City of Ontario, Cal. v. Quon, 130 S.Ct. 2619 (2010). The Supreme Court did not review the Ninth Circuit's conclusion concerning the existence of an expectation of privacy messages and mostly discussed the legality of the search, noting that "[t]he Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Quon*, 130 S.Ct. at 2629.

143. *Quon*, 529 F.3d at 898.

warrant. The court found that the wireless provider was an "electronic communication service" because it provided users with "the ability to send or receive wire or electronic communications" and that the storage of those messages was just a function of the main goal of sending and receiving them.[144] The court also concluded that an RCS was better represented by a company whose main function was to store or do advanced processing on information given them by their clients, unlike this wireless texting company.[145]

Theofel v. Farey-Jones is a controversial Ninth Circuit case that analyzed the term of protection of communications under the SCA.[146] In this case, email was obtained in the course of discovery during litigation with a "patently unlawful" subpoena.[147] The court held that emails stored on an electronic communications service (in this case, it was an Internet Service Provider) are protected by the SCA *indefinitely* if the storage is for the purpose of backup protection.[148] The court said that an "obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again."[149] This use of the ISP's services was found to "literally fall[] within the statutory definition" of the SCA's coverage.[150] The case demonstrates a certain level of arbitrariness in drawing the line between ECS and RCS facilities. The level of protection seems to hinge on a determination of primary purpose (communication or storage) rather on the actual service itself.

In the more recent case of *United States v. Warshak*, the Court of Appeals for the Sixth Circuit held that stored email was subject to the same Fourth Amendment protection as phone calls and letters.[151] Previously, the government was able to obtain emails with only a subpoena through the SCA, but this case held that strong warrant protection applied to email communication. By extending this right to email *stored* by an Internet Service Provider, the court changed how the SCA is applied and enforced. Whether this opinion will affect how the SCA is applied in other circuits remains to be seen. Possible changes to the SCA might also clarify its application to Cloud services.[152]

---

144. *Id*. at 901.

145. *Id*. at 902.

146. Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

147. *Id.* at 1071.

148. *Id*. at 1075.

149. *Id.*

150. *Id*.; 18 U.S.C. § 2510(17)(B).

151. United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010). In essence the issue is whether Cloud servers can be analogized to third-party owners of storage or similar facilities. Often this will depend in part on the terms of use of the service.

152. Probably the best example as of this writing is the Bill titled To Improve the Provisions Relating to the Privacy of Electronic Communications, S. 1011, 112th Cong. (2011)

For most consumers, however, the practical protection of their personal information in the Cloud (or absence thereof) is in the license and other end-user agreements. On the positive side, these agreements may give customers an idea of what to expect from the providers to which they are entrusting their personal information. Those agreements suffer from the usual flaws of contracts of adhesion, however. They tend to be more favorable to the provider that prepared the agreement than for the consumer, are typically non-negotiable, use dispute-resolution methods that may not be favorable to the consumer, and often offer very little in the way of methods to recover from damage to privacy, identity, or reputation caused by abuses by the provider. For example, the initial license agreement for Google Chrome web browser gave the company "a perpetual, irrevocable, worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display through" the web browser.[153] While this has since been modified to be less extreme, it demonstrates the sort of abuse of bargaining position that major Cloud service companies can try to exert over their users.

These agreements are often enforced through and are subject to state consumer protection laws. As such, abuse or misuse of personal information, can be considered a form of unfair or deceptive business practice. A good example of a state statute effectively cabining the ability of an end-user agreement to eliminate personal information protection is California's Online Privacy Protection Act of 2003 (OPPA). When it went into effect, it forced the providers of Cloud services to publish privacy policies on the front page of their websites as well as requiring that certain elements to be included in the policy. The statute also requires that the website maintain sufficient security measures to keep private information safe from intrusion.[154] While OPPA does not include any specific enforcement provisions, it can be enforced through the Unfair Competition Law, which is substantially equivalent to many states' unfair or deceptive business practices statutes.[155] OPPA was a good first step and a powerful example to other states. The statute

---

available at http://thomas.loc.gov/home/gpoxmlc112/s1011_is.xml, introduced by Senator Patrick Leahy (D-Vt) on May 17, 2011. The Bill would amend 18 U.S.C. § 2703 to require a warrant from a court of competent jurisdiction to obtain "disclosure by a provider of electronic communication service, remote computing service, or geolocation information service of the contents of a wire or electronic communication that is in electronic storage with or otherwise held or maintained by the provider."

153. Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575-22579 (2004).

154. *Id.*

155. Unfair Competition Law, CAL. BUS. & PROF. CODE §§ 17200-17209 (2004).

recognized the need of consumers to be (at least) informed about the use of their private information in order to protect themselves from potential abuses. The security requirement is also important. It may allow consumers to trust Cloud service providers, at least until the first major breach. Arguably, it makes that major breach less likely to occur.

The laws on the books provide some degree of protection, at least against wiretapping, and some deceptive practices in end-user agreements. In at least one appellate circuit, email is now protected as letters were when the notion of a reasonable expectation of privacy emerged. Yet neither courts nor legislators have fully embraced the extent to which everything about us will be in the Cloud, and the need for all of us to retain some control over access to and use of that information which, in aggregate, constitutes our societal identity. While the push toward the goal of each individual being in control of their own identity seems to be normatively agreeable, there are still important gaps to be filled and questions to be answered. The next section suggests ways to improve and deepen privacy in the Cloud.

B. Possible Ways Forward to Protect Personal Information in the Cloud

1. Federal Trade Commission Guidelines

In order to decide how best to improve the treatment of the personal information, the Federal Trade Commission studied the behavior of various entities in the United States, Canada, and Europe to see how they collect and use the information. The result is the Fair Information Practice Principles, a list of recommendations that acknowledge the importance of the goal to protect personal information.[156] The recommendations are articulated around five main principles:

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress[157]

Each of these principles is important in ensuring the protection of personal information, and each can be seen in various parts of the previous section. The notice/awareness principle is demonstrated in the enforcement of California's OPPA in making sure that consumers are

156. Fair Information Practice Principles, FEDERAL TRADE COMMISSION (June 25, 2007), *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

157. *Id.*

able to easily access a web site's privacy policy before personal information is given up. This principle is vital because it allows consumers to make an informed decision about what happens with their information. This notice should include not just the type of information that will be collected, but also who is collecting the data, what the data will be used for, who the potential recipients of the data are, whether releasing the data is voluntary or required, and finally what steps are taken to protect the data.

The Choice/Consent principle self-evidently goes hand in hand with Notice/Awareness. Once a consumer is aware of a company's policy, he or she can choose whether to agree to it or not. This is subject to the comments on contracts of adhesion, especially in cases where a particular Cloud service is in high-demand.

Access/Participation is not quite as obvious as the previous two principles. Though it is also very important, it is also probably the most often violated principle by Cloud services providers. The principle requires that an individual have "both access to data about him or herself—i.e., to view the data in an entity's files—and to contest the data's accuracy and completeness." A potential violation of this principle emerged in the discussion of targeted advertisements and targeted search results. It is all but impossible to verify what information is being held and used by search providers and their commercial partners.

Integrity/Security is a principle taken for granted by millions of individuals, for example whenever they do their banking in the Cloud. Most Cloud service providers realize that this principle is near and dear to the hearts of their users, and consequently they are likely to take steps (or to be seen to take steps) to provide security. The measures taken can include anything from increasing security of the physical servers to limiting password logins to increasing encryption when information is communicated.[158]

Enforcement/Redress is similarly essential because without it, it does not matter whether the provider complies with any other rules that are enforced by the policy.[159] If a consumer has no ability to enforce the

158. The most common form of this sort of protection is the HTTPS protocol (Hypertext Transfer Protocol Secure). The goal of this protocol is to create a secure channel for sending sensitive information over the Internet. It is commonly used for protecting credit card and banking information, but it could potentially be used on any normal website. HTTPS uses a public key/private key encryption scheme that allows the user to confirm that he wants to trust a certain site. After this confirmation, the information sent between the user and the website will be encrypted and safe from any other user who is "eavesdropping" on the network traffic.

159. The age-old debate of whether a law that cannot be enforced is actually a law has some part to play here. Also, the enforcement/redress should be able to properly match the vast difference in bargaining positions between the average user and a large, rich Cloud service provider. The threat of enforcement must be sufficient to influence the service provider not to violate the law.

privacy policy and to obtain redress when it is violated and this violation causes harm, then the policy is toothless as a legal matter. As such, it might be considered advertising (and possibly false advertising) rather than an enforceable contract.

The FTC does offer a forum for complaints against Cloud service providers. The Electronic Privacy Information Center (EPIC) has brought several complaints against various Cloud service providers in recent years, including a complaint against Google.[160] The complaint claimed that Google was misrepresenting the safety and security of information of several of its Cloud service sites, including Gmail, Google Docs, Google Desktop, and Google Calendar. EPIC alleged that, while the website professed the security of the services, there were many flaws that allowed unauthorized users access to documents, exposed user names and passwords to theft, and even security flaws that allowed others full control of a user's system. If these allegations were found to be true, then Google would not be following several different principles including Integrity/Security and Notice/Awareness.[161]

2. International Considerations

Another tool to look for answers and ideas about ways to protect personal information is to use a comparative approach and observe the laws and practices in other jurisdictions. Europe has a long history of strong privacy protection. Privacy is seen as an extension of the right to respect and personal dignity, consisting of mainly rights to one's image, name, and reputation, a bundle that German legal scholars refer to as the right to *informational self-determination*, that is, the right to control the sorts of information about oneself.[162] This theory of privacy is different than the one applied in the U.S., which promotes privacy as a derivative of the freedom to be left alone, rather than as a matter of personal dignity. We do not suggest that either theory is better. However, the European notion's normative anchors seem deeper and more convincing. It has undeniably resulted in a more unified and focused set of statutes and rules concerning the protection of personal information and makes

160. Mark H. Wittow & Daniel J. Buller, *Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime*, 14 J. INTERNET L. 1, 6 (2010).

161. The Federal Trade Commission is still reviewing EPIC's complaint about Google's unfair and deceptive business practices in representations made about their Cloud services. The FTC has stated that the complaint "raises a number of concerns about the privacy and security of information collected from consumers online." *See* Letter from Eileen Harrington, Acting Dir., Bureau of Consumer Prot., to Marc Rotenberg, President, EPIC; John Verdi, Counsel, EPIC; and Anirban Sen, Fellow, EPIC (Mar. 18, 2009), *available at* http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.

162. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161 (2004).

protection of foreign-owned information contingent on the presence of acceptable rules in foreign jurisdictions.[163]

It also informed the list of recommendations released in 1980 by the Organization for Economic Co-operation and Development (OECD) on the protection of personal information across borders.[164] This list of recommendations, which was closely mirrored by the FTC's principles, was entirely embraced by the European Union's Data Protection Directive. As such, unlike the FTC principles, the OECD recommendations are law in the 27 member countries of the European Union and any company that wishes to capture and move personal information into or out of a European Union country must abide by these seven principles:

- Notice - Individuals must be informed that their data is being collected and about how it will be used.
- Choice - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
- Onward Transfer - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- Security - Reasonable efforts must be made to prevent loss of collected information.
- Data Integrity - Data must be relevant and reliable for the purpose it was collected for.
- Access - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
- Enforcement - There must be effective means of enforcing these rules.[165]

The application of these principles includes American companies, which must abide by the principles under the US-EU Safe Harbor process in order to do business in any EU member country.[166] The European Union has thus taken a stronger stance in supporting the protection of privacy. Arguably, that stance is improving personal information protection in third countries where companies decide to comply with EU rules to be able to do business in the EU and where the

163. *See* Paul Lanois, *Caught In The Clouds: The Web 2.0, Cloud Computing, And Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29 (2010).

164. *See* ORG. FOR ECON. CO-OPERATION AND DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2002), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

165. *See generally* Directive 95/46/EC, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

166. *See* US-EU Safe Harbor Information, EXPORT.GOV, http://www.export.gov/safeharbor; Whitman, *supra* note 162.

EU rules might inspire local legislators.[167] By contrast, privacy protection in the United States seems more fractured and disparate.

CONCLUSION

The Cloud will not replace individual storage of files, including copyrighted material, but much more content will be streamed from the Cloud, and many of the personal files we create and use will be backed up there. The Cloud will be an increasingly appealing alternative to store and access content. This poses two major sets of questions: will the move to a recentralized architecture make control of digital files easier for copyright holders and governments? The Internet was a move from mainframe architecture to a decentralized network of hundreds of millions of computers. We are moving back to a much more limited number of servers, or server farms, owned not by Internet users but by intermediaries. Will privacy rules apply to those servers? Will it be easier to locate and delete copyrighted files? Will this really spur new business models? Those are the issues on which we tried to shed light.

Copyright control may indeed be easier, and recent efforts, such as the Anti-Counterfeiting Trade Agreement, continue to vindicate efforts to prevent any unauthorized access to copyrighted material. Whether this makes sense, as major right holders try to put the brakes on the most powerful distribution network ever invented, is an open question. It is similarly doubtful that copyright holders will regain control of distribution as they had when they were selling "units," such as compact discs and DVDs. The real control will be in the hands of intermediaries that will determine what you see, or at least suggest what one gets to read, listen to, or watch. Because of the oversupply of information and the finite amount of time one can devote to finding content that one values most, this role will be critical. It also makes the efforts to recreate scarcity using copyright even more strange. In breaking corporate distribution barriers, the Cloud can also empower creators from every country in making their material available and export their cultural memes to others. Business models remain unclear, but if truly successful ones emerge, they will necessarily involve intermediation.

Privacy will perhaps be the biggest challenge. The laws that apply to third party servers, including in terms of obtaining information by simple subpoena with or without the knowledge of the "owner" of the

167. Several non-EU countries have passed or are attempting to pass data protection laws that borrow from the EU Data Protection Directive. These countries include Mexico, *see* The Law on the Protection of Personal Data Held by Private Parties, *available at* http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010 (web site in Spanish), and Malaysia, *see* Personal Data Protection Act of 2010, *discussion available at* http://www.bnai.com/Malaysia2010/default.aspx, as well as others.

information that is disclosed to governments, are nowhere near the level of protection of a personal computer in one's home. As a technical matter, it sounds intuitively obvious that access to a few server farms operated by a number of key intermediaries wishing to maintain good governmental relations is not as secure. Our analysis shows that there are significant gaps in privacy protection and looks at proposed corrective reforms.