

**Remarks of Gigi B. Sohn, President, Public Knowledge
To the
17th Annual Oregon Connections Telecommunications Conference
“The Broadband Ecosystem: Living with the Cloud”
October 18, 2012
(as prepared)**

Good Morning. I want to thank Chris Tamarin and the conference organizers for inviting me to be here today. Of course I wish it were yesterday, because it was Mary Beth Henry Appreciation Day in Portland. I understand that Mary Beth suggested that you invite me here to be your keynote speaker. So you know who to blame after I'm done!

For those of you who don't know much about Public Knowledge, let me brief you a bit. We're an 11 year old nonprofit advocacy group based in Washington DC that fights for policies to preserve an open, universally accessible and affordable Internet. We think that the consumer should be in control of their Internet experience. You and me and millions of our friends around the world. We don't think the telephone and cable companies should be gatekeepers just because they control access to the Internet. And we don't think the big Hollywood studios and record companies should be Internet gatekeepers by abusing copyright laws and advocating for mandates on technology. So sometimes we are asking the government to actively intervene to promote openness, competition and universal

access. And sometimes (particularly when it comes to copyright), we are asking them to stay out.

That much of computing is now moving to what is referred to as “the cloud” does not diminish our concerns about the desire and ability of industry and government to engage in gatekeeping, and in fact, because there aren’t many rules of the road when it comes to cloud computing, those concerns are exacerbated. I’ll explain that more in a few moments, but since I am the first speaker in a conference dedicated to talking about “Living with the Cloud,” it might make sense for me to explain a little bit exactly what the “cloud” is.

What Is “the Cloud”?

In essence, the cloud consists of any and all applications and services hosted and run on servers connected to the Internet – servers and applications that you and I, the end user, do not have to maintain or support, and which are available from just about every Internet-connected device. Some examples include email provided by a website like Gmail, & Yahoo; so-called lockers for your data, like DropBox, SugarSync, Box.Net; applications like YouTube, Flickr, Facebook and online calendar services; and remotely stored media like Google Docs and Amazon cloud locker for TV and music.

If you are thinking to yourself that cloud services don't really sound all that new and different, you're right. Webmail has been around for a long time, and some of you might remember services like MP3.com from the 1990's, where you authenticated that you owned a CD to a company that kept a copy on its server. What's different now is the type and sheer volume of what is kept online. Basic applications like word processing, spreadsheets calendars, photos, movies, video games, you name it, are all available in the cloud. With the increase in data and services comes a need for terabytes of storage – hence the popularity of consumer and business services like Carbonite, which charge fees so you can back up all of your data.

It's gotten to the point where you barely need a hard drive to do computing. For example, both Google, with its Chromebook, and Hewlett Packard manufacture personal computers intended to work entirely in the cloud. While those devices both have hard drives, they are tiny, and are not able to hold locally the kind of data and applications that we might have on a desktop computer.

The Legal and Policy Challenges of Cloud Computing

The benefits of cloud computing are enormous. Consumers, businesses, and governments increasingly rely on cloud storage and services to reduce overhead

costs, increase efficiency, collaborate, and access files from virtually anywhere.

But challenges abound. As is often the case with new technologies, our laws and policies have not kept pace, leaving cloud service providers and their users open to legal liability, loss of access to data and other unforeseen problems.

So far, the application of existing law and policy to the cloud has been largely ad-hoc—important questions regarding user privacy, data security, and copyright infringement are being decided by judges on a case-by-case basis. This of course, leads to inconsistent results. Congress has not weighed in yet, and not surprisingly, the laws on the books do not adequately reflect the way technology works today. For example, the Electronic Communications Privacy Act (ECPA), which is intended to protect our wireline communications from government surveillance, was passed in 1986, before the public internet as we know it came into being, and its provisions, while they address storage, don't match today's technological reality. Similarly outdated is copyright law, which was last substantially revised in 1976. The Copyright Act gives ownership rights in every copy. So does that mean that someone should be liable every time she makes temporary copies like cached copies or bring up a copy of a document from RAM? This mismatch between old laws and new technologies like the cloud are sure to result in unintended consequences, and not necessarily ones we will like.

Copyright

Let me start with copyright – issues that are near and dear to Public Knowledge’s heart. A remote locker can be a file-sharing platform for copyrighted music, movies, and other media. As with every other technology, users will sometimes use lockers illegally – sharing copyrighted material without authorization and not within the exceptions provided by the law. But as we have seen with many new technologies that have come before it, the largest copyright holders are bypassing individuals who are allegedly acting illegally and suing the owners and developers of cloud services instead, or they are enlisting the government to do it for them.

You’d think that after decades of lawsuits against the VCR, the MP3 player and digital video recorders, each of which resulted in huge increases in their revenues, the major movie and record companies would realize that new disruptive technologies help, and don’t harm their business models. You’d be wrong.

The most prominent example of copyright infringement claims against a cloud storage provider involves Megaupload, a file storage service that is being

sued for criminal copyright infringement by the Department of Justice. The Justice Department's indictment asserts that the company's business model depended on people violating copyright and that it gave them incentives to do so, while charging subscription fees for watching video and placing ads in front of material it didn't own. In addition to indicting Megaupload and its flamboyant CEO, Kim Dotcom, the Justice Department seized Megaupload's website, causing millions of customers to lose their data.

While a number of respected legal scholars and other commentators believe the case against Megaupload is not strong, the very existence of this case has the potential to stifle remote storage innovation. Think about it - what company, after this all-out and by many accounts frivolous pursuit of Megaupload by the U.S. government, would take the risk of incurring such liability?

Of course, the whole practice of seizing domain names and taking down websites is chilling in and of itself. A little known provision in the 2008 PRO-IP Act (Prioritizing Resources and Organization for Intellectual Property Act) allowed the government to seize any and all assets used to engage in copyright infringement. Little did we know at the time that this law would be used to justify domain name seizures without notice or due process. So far, two of the

government's highest profile domain name seizure cases, involving a Spanish sports streaming service called Rojadirecta and a music blog named Djaz1, have fallen apart. But not after the domain names were seized for over a year, in both cases.

Imagine the damage to cloud services and the Internet if Congress had been successful in passing the notorious Protect IP and Stop Online Infringement Acts (PIPA and SOPA) of last year. Those bills would have allowed the Justice Department to seize domain names of foreign and domestic websites on the barest of evidence and with little due process. Worst of all, it would have required Internet intermediaries like Internet Service providers, search engines and domain name registrars to block access to so-called “rogue” websites – redirecting them to a webpage that the user did not request. As I'm sure most of you know, those bills stirred up a massive protest by companies, individuals and organizations unlike any I've seen in almost 25 years of doing this stuff. But if you don't think the major copyright holders behind PIPA and SOPA will try again, come talk to me in 6 months.

Ownership

Who actually *owns* the data on a cloud service is another copyright-related concern that the current law doesn't contemplate. To the extent that this issue is being addressed at all, it is in the terms and conditions, sometimes known as terms of service, set by the cloud service provider. For example, with regard to both Amazon Web Services and Google Drive, the user continues to “own” the data but also licenses or consents to its further use by the service provider. Google’s T&Cs state “[w]hen you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide licen[s]e to use, host, store, reproduce, modify, create derivative works, . . . communicate, publish, publicly perform, publicly display and distribute such content.” Amazon’s terms and conditions say that “[y]ou consent to our use of Your Content to provide the Service Offerings to you and any End Users.” While both companies seemingly allow the user to “own” the data, what does it mean that the respective companies will use your content to publish, publicly perform, or “provide . . . Service Offerings to you and any End Users”? It seems like you “own” your data, but you cannot control what the service provider does with it. That’s pretty limited ownership, and certainly a huge limitation on your own copyright in the works you produce!

Other important ownership questions remain unanswered. As files move around between the user's own storage system and the remote storage system, who owns the file? Does it matter that the data passes through the user's RAM when he or she accesses it, or does it only matter where the file sits?

Regardless of who owns the data, if the storage company goes out of business, all user files are deleted. There is no requirement otherwise. Laura Sydell of NPR reported that this happened to Abel Habtegeorgis, who unexpectedly lost his data when his cloud service shut down. Similar questions were raised in 2008 when Yahoo Music Unlimited shut down. Yahoo forced users to listen to the music they purchased on only one computer and if users changed operating systems, they would lose the files as well.

The uncertainty of who owns what in the digital world impacts a very important consumer copyright protection – the so called “first sale doctrine.” The first sale doctrine says that if I own something, I can do whatever I want with it – I can sell it, give it away or throw it in the trash, so long as I no longer maintain a copy. But there are two barriers to giving away or selling so-called “born digital” files. The first is that while under the law I have a right to distribute my digital files, the copyright law prohibits me from reproducing them. The second barrier

relates to what I discussed before - if I don't actually own what is in the cloud, and all I have is partial ownership or a mere license then I have nothing to sell or give away. My colleague Sherwin Siy wrote a great blog post on August 28 about what happens to your iTunes library after you die. While iTunes is not a cloud service, the same problems of ownership follow data in the cloud.

Telecom Issues

No speech of mine would be complete without discussion of my first love – telecommunications policy. And no speech of mine with a discussion of telecommunications policy would be complete without mention of data caps and network neutrality. Data caps rank very high on the list of threats to cloud services. Data caps are limits on what a person can do with their Internet connection before bad things happen. Those bad things can vary – overage charges, throttling, and in the case of Comcast and AT&T, you can get thrown off of your Internet service for exceeding the cap two months in a row.

Don't believe me? Then take the case of Andre Vrignaud, who lives in nearby Seattle. After hitting his 250 GB data cap two months in a row, Comcast banned Andre for one year. Andre's best guess as to how he hit the cap? Uploading data to a remote backup service. Many of you felt a twinge of guilt

when I mentioned remote backup service. You know backing up your data is a responsible thing to do, and backing it up remotely is the best way to keep it safe. But, for whatever reason, you haven't quite gotten around to setting it up yet. To his credit, Andre was responsible enough to set it up. And that is what got him kicked off the internet for a year. Remember, data caps are for combined download and upload.

Like Andre, anyone using a cloud computing service is at risk of hitting their cap, and relatively fast. If a 150 or 250GB cap sounds like a lot to you, think about all of the things you like to do with an Internet connection – Online backups, remote storage of media, uploading videos to YouTube or other websites, uploading photos, downloading Windows updates and online video games would all count toward a data cap and it starts to add up. The result is that you have to start to watch the meter and think – what thing that I like to do should I **not** do today. That isn't good for Internet users or cloud innovators.

And for what? When the nation's largest Internet Service Providers first rolled out caps on both wired and wireless services, they claimed that their purpose was to relieve congestion on their networks. But as you all know, congestion happens at a moment in time, like 8 at night when everyone is using their Internet

connection. But Vrignaud was backing up his data at 3 in the morning. Data caps are a blunt instrument that don't solve the congestion problem. When the ISPs realized that they couldn't continue to make the congestion argument with a straight face, they were forced to reveal the truth – data caps are simply a way to wring more money from consumers. It's price gouging, plain and simple.

Where does network neutrality come in? Again, for the uninitiated, net neutrality is the principal that the company that provides access to the Internet should not favor certain content, applications or services either with better quality of service or higher speeds. In other words – ISPs shouldn't pick winners and losers on the Internet – end users should.

After the FCC adopted fairly weak net neutrality rules in 2010, some ISPs decided that some applications and services should be subject to their caps, and some shouldn't. Take Comcast for instance – it exempts its own Xfinity app from its data caps when it sends broadband service to an Xbox360 or TiVo. All other video applications – Netflix, Hulu, YouTube, EPIX, are subject to the cap.

This is a net neutrality violation plain and simple, and there is no reason that similar cap discrimination couldn't apply to cloud services. Maybe Google wants to pay AT&T to ensure that its cloud services aren't subject to its cap. Time

Warner Cable just announced yesterday that it is starting a new cloud service for businesses. What if it decided that other cloud services would be subject to data caps but theirs would not? This kind of discrimination would greatly disadvantage new competitive cloud services.

Data Privacy and Security

The next policy issue I'd like to discuss is data privacy and security. And I will warn you – unlike copyright and telecom, which I eat, breathe and sleep 24-7, I am less familiar with this topic. So don't ask me any questions about it, ok?

But seriously, who can get access to your data in the cloud and when is an incredibly important question that cannot be ignored. Between the ECPA and the USA PATRIOT Act, government officials can easily get access to data stored in the cloud, without notice to the user, through subpoenas or something called “d” orders, which has a very low burden of proof. Remotely stored information is not as robustly protected as locally stored data under the ECPA. So users of cloud storage facilities are more susceptible to government snooping. For example, the New York District Attorney has so far successfully pursued a subpoena to force Twitter to turn over the personal account information of Malcom Harris, an Occupy Wall Street protester who was arrested on the Brooklyn Bridge in October

2011. After Harris challenged the subpoena himself, a federal district court judge ruled, incredibly, that Harris himself didn't have standing (or a right under the law) to contest his order, because, among other things, the information resided on Twitter's remote servers! And apropos of the ownership discussion earlier, the judge also said that because Twitter's terms of service gave Twitter a license to use Harris' tweets, Harris didn't own them. Twitter to its credit, fought the judge's decision, though it turned over Harris' information when faced with a large civil contempt fine. The standing decision is on appeal. Imagine the implications for privacy, due process and the 4th amendment protection against unreasonable searches and seizures should the judge's ruling stand!

Another data privacy concern is that not all remotely stored data is secured or encrypted. This increases the chance that information may be stolen through unsavory means by hackers. Security breaches happen, and not rarely, and can adversely affect users that rely on the service. Gmail and Google docs, Sony's online video game accounts, and even senior government officials have had their data hacked. Remember Anthony Weiner and his direct Twitter message to a Seattle woman featuring his groin? He may be the government's most infamous hacking victim.

Jurisdiction

The final issue I want to discuss cuts across all of the other ones, and that is jurisdiction. In other words, what country or state has legal authority over data in the cloud? This is another unanswered question, and it is critically important. It may be the case that multiple countries will claim jurisdiction over data, depending on where the user lives, or where the server storing the data resides. This has ramifications because different countries have very different copyright, privacy and data security laws. For example, Europe has much stronger privacy protections for online data than the US. That's great for consumers and not so great for companies like Google and Facebook. In the Megaupload case I discussed previously, the U.S. claimed jurisdiction based on Megaupload's "extensive" operations in the U.S., primarily because Megaupload (a Hong Kong-based company) owned servers in the U.S. However, New Zealand courts claim jurisdiction over Megaupload creator Kim Dotcom because he lives there. By the way, there is no such thing as criminal copyright laws in New Zealand – all copyright laws are *civil* laws. Hong Kong could also potentially have jurisdiction since the company is headquartered there. This jurisdictional battle, among other things, has hobbled the US's attempt to prosecute Kim Dotcom and Megaupload.

What's the Solution?

So I just gave you four policy areas where there is a palpable disconnect between the law and reality. So what's the solution? I really dislike talking about problems without also talking about how to solve them. But I have to be honest with all of you – these are very difficult problems, and any legislative effort to solve them will take many years, and in case you haven't heard, it's not easy to pass new laws in Washington DC these days.

The good news is that efforts to update our copyright, privacy and communications laws and policies are underway. Early next year, Public Knowledge will re-release its Internet Blueprint, which proposes actual legislative fixes to our copyright and telecommunications laws, including one that would shorten copyright terms, which is the source of most of our copyright problems. A second would make it clear that temporary copies like RAM and cached copies are not considered “copies” for the purposes of copyright liability. And another would make it clear that the first sale doctrine attaches to our born digital goods – that we own them, not merely license them. If you want to take a look at these and other proposals, go to InternetBlueprint.org.

Meanwhile, our friends at the Center for Democracy and Technology, a DC-based cyberliberties group, are leading a multistakeholder effort to reform ECPA

to make sure that the government cannot access our communications and data easily. Representative Zoe Lofgren of California just introduced a bill that would, among other things, amend ECPA to require government to seek a warrant to compel service providers to divulge the content of communications of users *and* for user information generally if requested in bulk. It would also require the government to seek a warrant to track a wireless communication device, like a cellphone.

Some of the other problems I discussed don't need legislative solutions – they just need courageous regulators, who appear to be in short supply. Public Knowledge has now asked the Federal Communications Commission 3 times to examine data caps and their impact on consumers, and it has filed a complaint alleging that Comcast violated the terms of its merger agreement when it acquired NBC when it exempted its own video service from its data caps. I don't expect this FCC to act on any of our requests, but this highlights the need for those who care about an open Internet to insist that whoever the next President is appoint an FCC Chair who will protect consumers. The Federal Trade Commission also has the power to act when it comes to consumer privacy and data security and ownership issues that arise when cloud services go bust.

This is where all of you come in. With the federal government either unable or unwilling to act, the only way we are going to get to affordable universal broadband in this country is through state and local action.

But the reality is that there are some things that the legislature and agencies cannot or will not fix, and that will be decided in either the courts or the court of public opinion. I don't know how the US Congress or the legislature of any other country or state can mandate who has jurisdiction over cloud services or the data in it. This will be something that law enforcement and international courts, like the International Court of Trade, will have to figure out. I also think data caps are more likely to be stopped by a massive consumer revolt than by any agency action. When more and more people start to get data overage charges in the hundreds and thousands of dollars, something will have to give. It's too bad that the state of broadband competition is such that people can't just up and switch to a provider that doesn't impose caps.

Conclusion

To conclude, as much as I am concerned about how some of the gaps in law and policy might affect cloud services and the Internet itself, I'm also excited about what an exciting time it is both for these services and these policies. For the

first time in the decade I've been doing copyright work, the debate over SOPA and PIPA has made possible a serious conversation about what kind of copyright protection makes sense in the age of computers. Cloud apps like Twitter and Facebook are putting the tools of democratic discourse in the hands of citizens of repressive regimes. And devices like smartphones and tablets, however imperfectly, are doing their part to close the digital divide – both the economic and the urban-rural digital divides. So while I will certainly warn you all to be aware of what is going on in Washington, in your state and local legislatures and in state and federal courts, I think we should also celebrate our role in helping this amazing communication system reach its full potential as a driver of creativity, innovation, free expression and economic growth. Thank you!