Written statement of

Kevin Werbach

Associate Professor of Legal Studies & Business Ethics,

The Wharton School, University of Pennsylvania

werbach@wharton.upenn.edu

Hearing on ECPA Reform and the Revolution in Cloud Computing

House Judiciary Committee,
Subcommittee on the Constitution, Civil Rights and Civil Liberties

September 23, 2010

Hearing on ECPA Reform and the Revolution in Cloud Computing
September 23, 2010

Written Statement of Kevin Werbach

Chairman Nadler, Ranking Member Sensenbrenner, and Members of the Subcommittee:

Thank you for holding this hearing on the important issues around privacy and cloud computing, and for inviting me to testify. I am an associate professor of Legal Studies at the Wharton School of the University of Pennsylvania, and the founder of Supernova Group, an independent technology consulting firm. As FCC Counsel for New Technology Policy in the Clinton Administration, and as a member of the Presidential Transition Team for the Obama Administration, I saw how government actions can positively or negatively influence technological development. In my work as a scholar, I examine how policies supporting open, interconnected networks promote benefits such as innovation, investment, job creation, free expression, and U.S. global competitiveness.

In considering reform of the Electronic Communications Privacy Act (ECPA) in the age of cloud computing, this committee and the Congress have an opportunity to update our legal regime to reflect major changes in the technological environment over the past two decades. My testimony highlights these developments. In particular, I will highlight four major changes since the passage of ECPA in 1986:

- The move from personal computing to connected computing.
- The evolution of the Internet to a ubiquitous global platform for information, communications, and commerce.
- The emergence of cloud computing, and the business drivers of its growth.
- The importance of online intermediaries to trust in the Internet ecosystem.

Reform of ECPA should be considered against the backdrop of these broader trends. In each case, legislation and other government decisions have influenced the business environment, and will continue to do so.

From PCs to Connected Devices

The quarter-century from the birth of the personal computer industry until 2000 marked the successful progress toward, in the words of Microsoft's original mission statement, "a computer on every desk and in every home." The second stage of the information age involves the transformation of those personal computers into connected devices. The model is no longer one computer per person, but many, in different locations, offering different form factors and functionality. Apple, for example, sells the MacBook, the iPhone, the iPad, and the Apple TV, all of which are powerful personal computing devices. Users are not expected to choose among them, but to use each in different situations, as well as to access connected services from other devices at work or elsewhere.

The explosion of mobile devices accentuates this trend. Fifteen years ago, mobile phones were a luxury enjoyed by a small percentage of Americans. Today they are ubiquitous. Those phones have also steadily increased in functionality, becoming powerful handheld computers. With continuing advances in computing capacity and improvements in mobile networks, this trend will only continue. Major wireless network operators are beginning to roll out fourth generation (4G) mobile networks, offering substantially greater data capacity. In addition, an increasing number of phones support local wireless connections through WiFi or other technologies.

The iPhone did not exist in 2006. Within five years, every mobile phone sold in the US will likely be what is today considered a high-end smartphone: a device capable of accessing Internet-based services and running applications. These phones will increasingly integrate cameras, location detection, accelerometers, touch screens, and other features. And they will support large application ecosystems, much as Microsoft's Windows laid the foundation for a vast personal computer industry. There are already over 250,000 iPhone apps, and a growing number on competing platforms such as Android and Blackberry.

The multi-device era is necessarily a connected era, because the devices draw upon the network to allow themselves to offer smaller form factors and lower prices. And it is necessarily a cloud computing era. When users access their data from many devices, that data must be stored remotely in the network or synchronized across the devices through the network. In particular, the growth of mobile smartphones and the newer classes of netbooks and tablets eliminates the traditional assumption that a personal computer is the repository of all a user's information and applications. File hosting and "software as a service" will become integral parts of the computing experience, rather than options.

The combination of a pervasive Internet, widespread adoption of mobile devices, and rapid growth of cloud computing generate business activity that is already significant and increasingly massive. Moreover, there are few Americans who will not have some of their personal data stored on remote servers by online intermediaries. Government action to promote trust in electronic commerce and legislation creating safe harbors for digital intermediaries played an important role in the growth of the Internet ecosystem over the past fifteen years. There can be little doubt that the Internet has been a major boon to innovation, investment, freedom, and other national goals. Congress must now consider how to ensure that outdated legislative and regulatory regimes do not undermine those benefits in the coming years.

The Evolution of the Internet

The Internet today is both an essential business tool and an integral part of daily life for the vast majority of Americans. Many of us still talk about the Internet as a nascent technology. In reality, it has been roughly fifteen years since the Internet and electronic commerce first reached the commercial mass market, following more than twenty years of gestation as a research network. Though it is still developing, the Internet is now a major, well-established platform for communications, entertainment, information, and commerce.

Every day, hundreds of millions of Americans use the Internet to check the weather, book travel reservations, look up recipes, buy gifts, read the news, chat with friends, check their bank accounts, reserve movie tickets, research medical information, share photos, track sports scores, look for jobs, look for dates, watch television shows, watch short videos, play games… and countless other common activities. Online chatter and social networks drive success of every major entertainment category, online information sources are having a dramatic effect on the media, online resources and fund-raising are decisive elements of major political campaigns, and online transactions represent an ever-growing share of virtually every form of commercial activity.

Over 240 million Americans, nearly 80% of the population, are now Internet users, according to Nielsen. Millions more have access to the Internet at work. And with over 285 million US mobile phone subscribers and widespread deployment of WiFi wireless hotspots, a majority of American adults already access the Internet through wireless connections, according to the Pew Research Center. That latter number is growing especially rapidly. Globally, there are two billion people online, and over five billion mobile phones in use, an increasing percentage of which offer Internet connectivity. The Internet is the mass medium of the 21st Century.

Even more significant than the size of the Internet today is how Internet usage has changed. In 1995, accessing the Internet meant initiating a dial-up connection through a modem attached to a personal computer, at speeds that required several seconds to download a single image file. Today, the vast majority of American Internet users have broadband access, an "always on" service roughly 100 times as fast.[1] Software and hardware have evolved to offer a smoother, richer, more sophisticated Internet experience. Personal computers and even packaged software applications now build in automatic updating and other communications functions, taking for granted an Internet connection as an integral part of the experience.

In 1996, when Congress passed the Communications Decency Act, there were approximately 100,000 websites in existence; today there are well over 100 million. In 1998, when Congress passed the Digital Millennium Copyright Act and the Internet Tax Freedom Act, Google had not yet been founded. In fact, virtually none of the top 100 sites on the Web today were in existence at that time.[2] Facebook, the most popular site on the Web today, was only launched in 2004. Today it has over half a billion users worldwide. I could cite many other examples. The point is that the Internet of 2010 is not the Internet fifteen or ten or even five years ago. And the Internet of 2015 or 2020 will diverge even further from the past.

Rise of the Cloud

As the external usage of the network has changed, the internal components have evolved as well. Cloud computing is an approach that places application processing and storage in network based data centers rather than solely in end-user devices such as personal computers. There are many definitions of cloud computing, but experts agree on one thing: this shift to network-based functionality will have massive business impacts. As John Hagel and John Seely Brown of Deloitte's Center for the Edge recently stated, "Cloud

[1] A February 2010 FCC survey found that 78% of American adults are Internet users and 65% have home broadband access. *See* Broadband Use and Adoption in America, John B. Horrigan, OBI Working Paper No. 1, at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296442A1.pdf.

2 *See* The 1000 Most-Visited Sites on the Web, *at* http://www.google.com/adplanner/static/top1000/.

computing has the potential to generate a series of disruptions that will ripple out from the tech industry and ultimately transform many industries around the world."[3]

Fifteen years ago, many websites resided on a single server computer. Even very popular sites might only have a handful of servers fed by "load balancing" software at a single location. Today, the leading Internet companies build massive, multi-billion dollar data centers the size of several football fields, each housing thousands of networked computers. A major service provider such as Google has more web-connected servers than the entire Internet fifteen years ago, all linked into a colossal virtual supercomputer. And Google is at the leading edge of a huge trend. Smaller providers such as Twitter are building their own data centers, while others tap into "public clouds" offered by companies such as Amazon.com.

The rise of smart connected mobile devices further feeds this trend. Due to their small size, mobile phones do not have the same storage capacity as personal computers. Even when used for services such as email or document review, they are almost never a user's sole computing device. Rather, provide a mobile "window" into the user's data. As a result of these two factors, virtually any application involving significant amounts of user data on mobile devices will incorporate remote storage and a cloud computing architecture. This is equally true for mobile access to a consumer service such as iTunes for music or Yelp for local restaurant information, as for business applications such as Salesforce.com or Google Docs.

The momentum toward cloud computing is strong. A solid majority of experts participating in a recent Pew Foundation Future of the Internet Survey expected that in a decade, most people will access software applications and share information through remote servers rather than desktop applications.[4] Cloud computing involves much more than a few high-profile applications such as GMail and Salesforce.com. Startup companies increasingly rely on public clouds provided by vendors such as Amazon.com in lieu of building and maintaining their own server infrastructure. At the other end of the spectrum, large online service providers as well as enterprises with their own existing data center infrastructure are all potential or actual cloud computing providers.

The business case for cloud computing is based on three core benefits.

First, there are significant economies of scale in delivering application functionality through large remote data centers. Service providers can operate, configure, and update a centrally-managed collection of resources more efficiently than individual users responsible for their own personal computers. Backup, business continuity, security, and other utility functions are significantly more efficient if deployed across a large virtualized cloud of computers. The cost is shared across all the customers, and the cloud provider can develop expertise beyond that of individual companies.

[3] John Hagel III and John Seely Brown, Cloud Computing's Stormy Future, HBR Blog, September 14, 2010, *at* http://blogs.hbr.org/bigshift/2010/09/cloud-computings-stormy-future.html.

[4] Janna Quitney Anderson and Lee Rainie, The Future of Cloud Computing, Pew Internet and American Life Project, June 11, 2010, *at* http://pewresearch.org/pubs/1623/future-cloud-computing-technology-experts.

Second, because it allows many users to share large utility computing clusters, cloud computing is a better solution when demand fluctuates. Consider a startup launching a new web-based service. It has to ensure that it has enough processing and storage capacity to meet user demand. If the company must provision servers itself, there may be a substantial cost and delay to increase capacity when it under-estimates demand. And if the company over-estimates demand, it will spend unnecessary resources provisioning servers that it doesn't use. In one case, the service may crash, and in the other, the company wastes money. Neither is an attractive outcome. Moreover, demand forecasting is a constant exercise. What if the company runs a special promotion that causes a short-term spike in usage? Or what if it offers an enterprise service that is lightly used on the weekends? There is no way for any individual company to match supply and demand efficiently.

In a cloud computing environment, on the other hand, companies share virtual capacity in massive clouds. The scale of the cloud platforms makes capacity a commodity for the provider, so overprovisioning is not the same difficulty as for individual companies. The cloud provider can also deploy virtualization software and other technical mechanisms to more efficiently utilize its capacity. Aggregation of demand across different services with different requirements naturally tends to smooth out spikes. Especially in a fast-changing environment, the cloud approach therefore provides a more efficient and higher performing solution than companies could provide through local self-provisioning.

Third, cloud computing allows the service provider to capture and aggregate large volumes of user data. This information can help the service provider improve its service, or it can open up new business opportunities. Gmail, which generates revenue through targeted advertisements, is a good example. Google does not need to charge for its email service, even though the gigabytes of storage it provides to users are not costless to provision. Instead, Google monetizes Gmail by algorithmically matching message text to targeted advertisements. Only because Google can aggregate large numbers of ads and large volumes of email text in the same computing environment as its analytical software can it make this model work.

From a pricing standpoint, cloud computing overcomes many of the problems with traditional software business models. It produces recurring revenue streams, which are often more attractive than one-time payments. It allows customers to "pay as you go", without substantial up-front costs, and to scale up or down their financial commitments as needed. For businesses, cloud computing represents a shift from computing services as a set of capital expenditures – servers, bandwidth, software licenses, software maintenance, IT staff, etc. – into a payment analogous to other utilities such as electricity and water.

Cloud Providers as Intermediaries

In the early days of e-commerce, there was much enthusiasm for the concept of disintermediation. Rather than operate through a middleman such as a retail store or an insurance agent, a supplier of products or services could use the Internet to interact directly with its customers, cutting costs and improving efficiency along the way. To some extent this has been the case, but the disintermediation story is incomplete. The Internet in fact creates and depends upon a new set of digital intermediaries. The oceanic quantity of information available online overwhelms the ability of any user to find the most relevant, highest quality resources on their own. Online intermediaries can perform these functions and add additional value in the process.

Search engines were the first prominent online intermediaries. Users can connect to any website directly, but it takes the incredibly sophisticated analytics and massive computing power of sites such as Google and Bing to sift in real time through billions of pages and show the user where to find what they were looking for. E-commerce sites such as eBay and Amazon.com also function as intermediaries, not only processing transactions, but offering features such as ratings, recommendations, wish lists, and other functions beyond the capability of any physical world retailer. Facebook knits together social networks and provides hosting for billions of messages, photos, videos, links, and other materials. Paypal offers payment processing functionality so that virtually any online business can access payments efficiently from users around the world.

The companies in these examples have gone even further by establishing application programming interfaces (APIs) to allow other providers to plug into their platforms. Consider a company such as Zynga, a developer of social games. It operates largely on top of Facebook, rather than as a standalone website. By leveraging Facebook's massive user base, development tools, and social networking tools, Zynga quickly developed a string of massively successful games. It reportedly will generate $500 million in revenue this year, its most recent venture capital funding valued the company at well over $1 billion, and it is on track for an initial public offering. Zynga is an intermediary for tens of millions of players, but it is an intermediary that itself connects to other intermediaries such as Facebook and PayPal. The relationships between those providers necessarily involve sharing of user data.

Online intermediaries therefore necessarily raise important privacy and security questions. The growth of cloud computing will bring these issues to the forefront. By its very nature, cloud computing requires users to give up physical control of their data, and allow it to reside on the remote infrastructure of an intermediary provider. This applies to both the identity information about who the user is and where information is being transported, as well as the content of that information. While there are technical mechanisms to secure that data, it is the service provider, not the user, that must implement them. Users in many cases will not even realize that their data is sitting on remote servers and subject to inspection or distribution. Cloud computing makes distributed processing transparent to the end-user, so a user may have no indication that her data is no longer sitting on her PC, but on a rack of servers far away.

A smooth transition to cloud computing requires users to continue feeling a sense of trust online. In the early days of e-commerce, users hesitated to give their credit cards to websites. The idea of typing this information into a machine seemed scary. Concerns about fraud held back the growth of e-commerce. It was only through a combination of technical measures to secure information, adoption of best practices in part through government prodding, and gradual development of user confidence that this hurdle was overcome. Every time an ordinary American ordered a book on Amazon.com or bought a collectible on eBay and got what they paid for, their trust in the Internet increased a little bit. Even more important, that American's friends and family saw the same thing. The gradual accumulation of positive experiences, and the relative paucity of negative experiences, brought the Internet to its current point of mainstream acceptance.

If circumstances change, this trust could unravel. At the margin, users will choose to engage more or less actively online based on their own experiences and those of their friends and families. Already, the large amount of personal information regularly shared on social networks has produced sharp concerns in many quarters. Though it is fashionable to assert that today's young people are unconcerned about privacy, research shows that in many ways they feel even more strongly about the need to control their personal information than their elders.[5]

Users care about protection of their data, and will change their behavior if they feel the protections are insufficient. Some users will switch to more secure providers, some will use encryption to make their data less visible, some will keep more data locally even when the cloud architecture provides clear benefits, and some will simply engage in less activity online. All of these actions will be based on incomplete information and colored by confusion or inaccurate rumors. In other words, a drop in trust in online intermediaries will have unpredictable results, but will inevitably add greater friction to the Internet economy. That friction will be a drag on the continued growth of online activity, and all the benefits it brings.

One important reason for the level of confidence about Internet privacy is an implicit deal embedded in several key Internet-related statutes. The essence of this deal is that service providers avoid intermediary liability in return for a commitment not to meddle with user information, and to establish orderly procedures for access when sought for legitimate purposes such as law enforcement and stopping copyright infringement. This structure underlies the safe harbors in Section 230 of the Telecommunications Act of 1996, as well as Section 512 of the Digital Millennium Copyright Act. It represents an extension of the common carriage mechanism that historically applied to telephone companies, and data privacy restrictions that Congress imposed on cable television providers.

The safe harbor approach is valuable because it provides confidence for all the potential parties. A user has confidence that if she makes information available to an online service provider, that information won't be accessed inappropriately. The service provider has confidence that it won't accrue legal liability for the actions of its users. Given the enormous scale and velocity of online information flows, any regime requiring online providers to monitor or approve user activity beforehand is likely to be infeasible. Investors will hesitate to fund business models when massive liability could undermine a profitable business. Finally, law enforcement and other outside parties such as copyright holders have the confidence that service providers will provide them access to necessary information, subject to an appropriate process.

If user data stored in the cloud is not subject to appropriate protections from unauthorized access, trust in cloud computing could be undermined. This is true whether the access is by private or governmental actors. The fallout from a loss of trust in the Internet would be felt not only by companies that provide cloud-based services, but by the much larger community of businesses they connect to, and by users themselves. In considering ECPA reform, this committee should consider not only the appropriate balance between the needs of law enforcement and protection of civil liberties, but also the effects of its decisions on the health of the Internet ecosystem.

[5] *See* danah boyd and Eszter Hargittai, Facebook Privacy Settings: Who Cares?, First Monday, August 2010, *at* http://www.danah.org/papers/2010/FM-FacebookPrivacySettings.pdf; Mary Madden and Aaron Smith, Reputation Management and Social Media, Pew Internet and American Life Project, May 2010, *at* http://www.pewinternet.org/Reports/2010/Reputation-Management.aspx.

Conclusion

The health of the Internet should be a national priority. Most of the greatest Internet startup success stories are based here in the U.S., and American businesses and consumers have benefitted immensely from the growth of our Internet economy during the past two decades. Cloud computing represents a new stage in the evolution of that economy. U.S. Internet leadership stems in part from our success in implementing "a predictable, minimalist, consistent and simple legal environment," in the words of the 1997 *Framework for Global Electronic Commerce*. However, the solutions of the past may not be the best ones for the present or the future. Keeping old rules in place may actually create inconsistency and uncertainty. It is incumbent upon Congress and the other arms of the Federal Government to consider how to achieve legitimate public policy objectives consistent with the fast-changing technological environment.