# The Contrasting Environments for Cloud Computing In the United States and Europe: Jurisdiction and Contrasts

Brock Rutter

Faculty of Law
McGill University
Montreal, Canada

April, 2012

**A thesis submitted to McGill University in partial fulfillment of the Requirements of the degree of Master of Laws (LL.M.)**

## ABSTRACT

[Le Résumé français suit.]

This thesis will first offer an explanation of what “the cloud” is and why it matters to us. It will also detail some ways in which law can both alleviate and exacerbate problems in the cloud. Subsequent sections will contrast regulation in the United States and Europe, which were selected as examples because of the contrasts they offer. A section on jurisdiction will outline the ways in which cloud providers can be subject to numerous regulatory regimes simultaneously. This section should show how governance of the cloud has necessitated new and permissive theories for the exercise of jurisdiction; what constraints there are derive instead from real-world limitations on enforcement and providers’ decisions whether or not to operate in each jurisdiction. Finally, important reasons exist to retain the global nature of the cloud computing network even if equally valid reasons exist for allowing nations to make different policy decisions in areas affected by cloud computing. A globally interoperative network need not mean conversion of substantive law nor undue restrictions on the locations of infrastructure.

## RÉSUMÉ

Ce mémoire commence par offrir une explication de ce en quoi consiste l'informatique en nuage et de son importance pour nous. Il montrera en quoi le droit peut à la fois atténuer et aggraver les problèmes dans le nuage. Les sections suivantes opposeront la réglementation aux États-Unis et en Europe, qui ont été sélectionnés à titre d'exemples en raison des contrastes qu'elles offrent. Une section sur la compétence donnera un aperçu des façons dont les fournisseurs des services de l'informatique en nuage peuvent être soumis à de nombreux régimes réglementaires simultanément. Cette section se donne pour but de montrer comment la gouvernance du « nuage » a donné lieu à de nouvelles théories permissives pour l'exercice de la compétence juridictionnelle, les contraintes découlant plutôt du monde réel sur la mise en œuvre et les décisions des fournisseurs d’exercer des activités ou non dans chaque système juridique. Enfin, il existe d'importantes raisons de conserver le caractère mondial du réseau informatique en nuage, même s’il existe aussi des raisons valables pour permettre aux nations de prendre des décisions politiques différentes dans les domaines touchés par le cloud computing. Un réseau mondial interopérationnel ne se traduit pas nécessairement par des changements au droit substantif ou des restrictions indues sur l’emplacement des infrastructures.

## ACKNOWLEDGEMENTS

I wish to thank the following people for their assistance: First, my advisor Prof. Frédéric Mégret for his assistance and constructive. Secondly, Oliver Goodenough of Vermont Law School and Harvard's Berkman Center for Internet and Society for starting me on the path that eventually lead to this subject. I have also benefited from my periodic association with the Berkman Center and specifically the Cloud Research group. I also owe a debt of thanks to attorney Irving Handelman of Montreal who gave generously of his time in reading and commenting on a draft of this paper. Finally I am also grateful to my wife Nicole who has been not only offered editing assistance and also for her support at home.

**Table of Contents**

## 1 INTRODUCTION

### 1.1 The continuing importance of territorial jurisdiction

The metaphor of "the cloud" was originally meant to describe the performance of computing tasks in some other, indeterminate place. However, all computing tasks – even those outsourced to the cloud – must take place in some location. Likewise, users of cloud services reside in determinable locations. Both the location of cloud infrastructure and the location of cloud users have importance legal consequences. Despite an initial enthusiasm for the Internet as being somehow apart from traditional notions of territory, jurisdiction has very much come to the cloud.

Increasingly, the cloud is hosted in new purpose-built data centers; these structures are not the only things binding the cloud to earth; national boundaries are also being transplanted into the cloud, producing experiences that differ for users based on the jurisdiction from which they access the cloud. The United States and the European Union, respectively the biggest and second biggest cloud computing markets exhibit stark contrast in their respective laws bearing on cloud computing, including privacy regulation and consumer protections. In the important realm of privacy regulation, much of the rest of the world is falling in behind the European model, such that the United States is increasingly the global outlier.[1]

An initial wave of Internet exceptionalism has given way to an acceptance that jurisdiction still matters in the cloud, even if it does so in ways that are dramatically different from the pre-Internet era. Jurisdiction over the cloud is different both because cloud providers target many countries at once, potentially themselves in numerous locations. This means that cloud

[1] See, Abraham L Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Ithaca, NY: Cornell University Press, 2008) at 104("With the notable exception of U.S. citizens, consumers across the globe increasingly enjoy enforceable rights of consent, notice, and access to personal information collected in the public and private sectors.")

providers are subject to often conflicting legal demands from various countries, and their actual conduct is governed by the reference to which regimes have the actual power to enforce their norms. Jurisdiction is relevant in at least two ways; it can refer to the location of customers targeted by cloud services or also to the location of infrastructure such as data centers. However, regulatory regimes based upon the location of end users should not unnecessarily impact on the location of cloud infrastructure.

This thesis will first offer an explanation of what "the cloud" is and why it matters to us. It will also detail some ways in which law can both alleviate and exacerbate problems in the cloud. Subsequent sections will contrast regulation in the United States and Europe, which were selected as examples because of the contrasts they offer. A section on jurisdiction will outline the ways in which cloud providers can be subject to numerous regulatory regimes simultaneously. This section should show how governance of the cloud has necessitated new and permissive theories for the exercise of jurisdiction; what constraints there are derive instead from real-world limitations on enforcement and providers' decisions whether or not to operate in each jurisdiction. Finally, important reasons exist to retain the global nature of the cloud computing network even if equally valid reasons exist for allowing nations to make different policy decisions in areas affected by cloud computing. A globally interoperative network need not mean conversion of substantive law nor undue restrictions on the locations of infrastructure.

### 1.2 Diversity of approaches between the U.S. and EU

Different countries have taken different routes to "the cloud". As the global network grows it does so in markedly different legal environments. While the United States and Europe are respectively the biggest and second biggest cloud computing markets, the differences between them in the law bearing on cloud computing are stark.[2] As with the theory of the "law of the

[2] See,Kevin J O'Brien, "Europe Turns to the Cloud", *The New York Times* (24 July 2011), online: <http://www.nytimes.com/2011/07/25/technology/europe-turns-to-the-cloud.html>.

horse", there is perhaps no "law of the cloud" per se.[3] Data protection law, libel, privacy protection, consumer protection law, competition law, and others affect cloud computing. Standards and procedures for access to information by civil litigants and law enforcement vary widely by country as well.

### 1.3 Overlapping jurisdiction and conflicting laws

Because of the trans-national nature of cloud computing and the Internet which supports it, jurisdictional questions are also difficult. Countries can claim jurisdiction based on a number of factors, including the location of servers and other infrastructure, users, parent companies, or target markets. Many nations, notably EU member states and the United States, project laws that have significant extraterritorial effects. Because of this real-world situations exist from time to time where providers or users face conflicting legal demands.

The substantive and jurisdictional law related to the cloud will remain difficult and inharmonious for some time. In the meantime, cloud users and service providers carry on under legal regimes that not only vary significantly by country but sometimes overlap. Jurisdictional concerns and incompatibilities could exert pressure toward fragmentation of the cloud along national borders. This could damage the very global-ness that is an essential feature of the cloud.

[3] Frank H Easterbrook, "Cyberspace and the Law of the Horse" (1996):1996 University of Chicago Legal Forum 207, online: <http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf>;

But, see, Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach" (1999) 113 Harv L Rev 501, online: <http://www.lessig.org/content/articles/works/finalhls.pdf>.

## 2 THE POWER OF THE CLOUD

### 2.1 What is the cloud?

Cloud computing is the use of computing power situated away from the end user, which generally produces the illusion that processes happening at a remote location are happening on the computer. Important for the end user too is also the illusion of infinite scalability – the ability to add or subtract computing power at will. The term "the cloud" is derived from the practice of depicting the Internet or the network as a cloud on computer schematics; a cloud icon would often be used to depict processes going on somewhere else, the exact location of which was not of immediate concern to the user.

The U.S. National Institutes of Standards and Technology definition of cloud computing may be helpful.

> *Cloud computing is a model for enabling ubiquitous, 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.*[4]

The NIST definition goes on to describe the essential characteristics, service models, and deployment models. The essential characteristics are; on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The service models are; software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Software as a service provides the most finished product to the end-user, whereas infrastructure as a service leaves the most flexibility but also most work to be done to the end user. Software as a service is basically indistinguishable from an application installed on a user's computer. For example, there is little to indicate that Google Docs or even Facebook is

[4] Peter Mell & Timothy Grace, *The NIST Definition of Cloud Computing* (Washington, DC: National Institute of Standards and Technology, 2011) online: < http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

not running "on" the user's computer but rather in the cloud. At the other extreme, infrastructure as a service models rent out raw computing power or storage space. IaaS would be useless unless the user supplied the software applications to run on it. Amazon provides IaaS computing power in the form of EC2 and IaaS storage in the form of AWS. In the mid-point of the sliding scale, platform as a service provides some building blocks for customization. For example, Google App Engine allows programmers to design their own apps. The average casual consumer is much more likely to come into contact with SaaS than the other two varieties. However, services can also be layered on each other. Dropbox provides SaaS to consumers but rents IaaS services from Amazon.[5]

The deployment models include;

> ***Private cloud****. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.*
>
> ***Community cloud****. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.*
>
> ***Public cloud****. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.*
>
> ***Hybrid cloud****. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).*[6]

An alternate view describes cloud computing in roughly similar terms;

> *Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand.*

---

[5] W Kuan Hon, Christopher Millard & Ian Walden, "The Problem of 'Personal Data' in Cloud Computing - What Information Is Regulated? The Cloud of Unknowing, Part 1" (2011) SSRN eLibrary, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577> at 5–6.

[6] Mell & Grace, *supra* note 4 (NIST Definition).

> *Services (especially infrastructure) are abstracted and typically virtualised, generally being allocated from a pool shared as a fungible resource with other customers.*
>
> *Charging, where present, is commonly on an access basis, often in proportion to the resources used.*
>
> *Cloud computing activities are often classified under three main service models – Infrastructure as a Service ('IaaS'), Platform as a Service ('PaaS') or Software as a Service ('SaaS'). These services form a spectrum, from low-level (IaaS) to high-level (SaaS) functionality, with PaaS in between.*[7]

A narrower view is possible;

> *Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds..*[8]

So-called private clouds – when companies build their own cloud- infrastructure – do not raise all the issues that otherwise pertain to cloud computing.

### 2.2 Ending the desktop era

Many of us are more familiar with a model in which software is installed directly on a computer. For example, a word processing program such as Microsoft's Word can be installed and run on a user's laptop. The program is stored and run directly from the computer, and all

[7] W Kuan Hon, Julia Hornle & Christopher Millard, "Data Protection Jurisdiction and Cloud Computing - When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3" (2012), online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240> at 3.

[8] Michael Armbrust et al, *Above the Clouds: A Berkeley View of Cloud Computing* (Berkeley: University of California at Berkeley, 2009) at 3.

of the information necessary to run it exists solely on the computer. However, since 2011, Microsoft now offers its Office 365 suite, a cloud-based version of the popular Office suite, which includes Word. When users turn to the cloud-based Office 365 the actual computing takes place not on the user's computer but in a Microsoft data center somewhere else. Depending on a number of factors, including the user's location and the need to balance workloads, the tasks could be sent to any one – or more – of Microsoft's data centers around the world.[9] The importance of cloud services is growing for businesses. Microsoft – a company famous for putting "a pc on every desk" – now makes more money per user from its cloud based Exchange email service than on the traditional model where clients maintain their own servers. At the same time, the final cost to the end user is less.[10] The company that defined the PC era has embraced the cloud, widely seen as the harbinger of the post-PC era. According to CEO Steve Ballmer, "It's the next step, it's the next phase, it's the next transition…"[11]

Microsoft's Office 365 is along with its competitor Google Docs a software-as-a-service offering. Software-as-a-Service, or SaaS, is one of the three commonly accepted delivery models of cloud computing alongside Platform-as-a-Service ("PaaS") and Infrastructure-as-a-Service ("IaaS"). The different modes of service delivery are described more below and differ primarily as to the level of customization available to the end user. SaaS users plug in to applications designed by providers with very little, or no customizability. IaaS users are provided with a much cleaner slate by their cloud providers, renting "instances" of "virtualized" computers on which they must install or build their own software, a prominent example being Amazon's popular EC2. In

[9] Rich Miller, "Microsoft Picks Virginia for Major Data Center » Data Center Knowledge", *Data Center Knowledge*, online: <http://www.datacenterknowledge.com/archives/2010/08/27/microsoft-picks-virginia-for-major-data-center/>.

[10] Jon Brodkin, "Microsoft: We make more money on cloud-based Exchange | Asia Cloud Forum", (16 August 2011), online: *Asia Cloud Forum* <http://www.asiacloudforum.com/content/microsoft-we-make-more-money-cloud-based-exchange>.

[11] Steve Ballmer, *Cloud Computing* (Paul G. Allen Center for Computer Science & Engineering, University of Washington, 2010), online: < http://www.microsoft.com/presspass/exec/steve/2010/03-04cloud.mspx>.

the middle, PaaS users are provided with slightly more structure and programming environments meant to support certain computing languages.[12]

The shift from computing on a user's computer to in a remote data center means many things. Drastically less computing power is required of the user's computer. More than just computing power is outsourced, however. In the case of an enterprise program like Exchange, this means the company need no longer maintain its own server, cool it, and staff it with in-house IT staff.[13] Program updates are pushed to the user automatically, whether for a new version of iTunes or a new enterprise-level email system. Taken to the extreme, cloud-based computing systems could completely hollow out the client computer. At this point the computer on your desk or lap, or tablet in your hands would be only a portal to services elsewhere. It would require only an Internet browser and a dependable connection to the Internet. Google is working on just such a product with its Cr-48 computers running the Chrome operating system. The operating system, which shares its name with Google's web browser, is "about as stripped down as you can get." Users install no additional hardware and all storage is in the cloud. The system has been tested with a small number of developers and journalists and should launch soon.[14]

### 2.3 Outsourcing our computing tasks

By moving more and more functions to the cloud, the power of the local computer becomes less and less relevant. Amazon has recently taken reliance on the cloud to a new level with its Silk operating system for the new Kindle Fire. The system emphasizes not the computing power it puts in users' hands, but the coordination of what is on the local tablet with the computing power available in the cloud. The Kindle Fire is Amazon's entry into the full-feature tablet

[12] "Amazon Web Services",, online: <http://aws.amazon.com/>; "Google Apps for Business | Official Website",, online: <http://www.google.com/apps/intl/en/business/index.html>; "Google App Engine — Google Developers",, online: <https://developers.google.com/appengine/>.

[13] This creates the possibility of in-house IT departments as built-in constituencies against cloud adoption.

[14] Duncan Gere, "Spending a week with Chrome OS - Chrome OS review & test (Wired UK)", *Wired UK*, online: <http://www.wired.co.uk/news/archive/2011-04/4/a-week-with-chromeos>.

market, intended to compete with the Apple iPad – at less than half the cost. By putting more of the functions of the tablet "in the cloud", Amazon is able to offer full functionality on a much cheaper stripped down device.

> *Silk takes into consideration both the computing power in the user's device and the computing power in Amazon's enormous data centers, then executes tasks for maximum efficiency…. For a long time, most programming problems were defined by how much processing power you had. That's why you used to hear so much about powerful chips and now you don't. With the advent of the cloud, the amount of processing power for most problems isn't the issue; correctly apportioning tasks and making millions of servers work together is.*[15]

More and more, computing tasks are being performed not at the place where they are accessed but at centralized locations that offer advantages of scale, dependability, or access to data. Examples range from major big business enterprise functions of all sorts from vendors such as Salesforce, Rackspace, Google, and others down to other handheld devices. Apple's Siri personal assistant function on every newer iPhone communicates with centralized processing run by Apple, as do Google's Android products, as well as Microsoft's new smartphone line, the newest entrant into the market. The cloud model makes it unnecessary to equip each and every device with all the computing tasks asked of our newest devices. It also allows for economies of scale in computing tasks and the creation of centralized data banks.[16]

### 2.4 "Utility computing" – The electricity metaphor

Proponents hope that computing power will become a utility, something we can plug in to, and access as effortlessly as other utilities. In a metaphor popularized by business and technology writer Nicholas Carr, computing is compared to electricity.[17] The manner of powering factories was once a differentiating characteristic of some factories over others – a competitive

---

[15] Quentin Hardy, "Amazon's Silk Browser Plays Another Role", *New York Times* (28 September 2011), online: <http://bitsblogsnytimescom/2011/09/28/amazons-silk-browser-plays-another-role/>.

[16] Systems such as Siri and most Google services "learn" based on the behaviour of their users.

[17] Nicholas G Carr, *The Big Switch: Rewiring the World, from Edison to Google* (W. W. Norton and Company, 2011).

advantage. A man named Henry Burden in upstate New York once ensured the competitive advantage of his ironworks factory by building a waterwheel that was bigger and better than those of his competitors. The wheel was not electric, but rather the power source for an unusually large, powerful, and efficient system of "millwork" that powered the machines in his factory by a system of pulleys.[18]

The ongoing evolution in the world of computing has important similarities to the evolution of information technology. Each was first a rarity by which a firm could gain a competitive advantage, and is now becoming commonplace and a commodity input. Within a few years after Burden built his waterwheel, electricity had become the dominant power source; waterwheels were completely obsolete. Electric power plants were at first an amazing novelty, and at first nearly every plant had its own. Eventually, however, the utility model won out and now nearly every home and business buys its own power from a commercial producer. Each power source is roughly equal and no business secures a competitive advantage over others through its power source.[19] Information technology has followed a similar trajectory. In a previous book, "Does IT Matter?" Carr chronicled the decline of IT as a competitive advantage.[20]

Far from being a bad thing, this erosion of the IT competitive advantage levels the field and lets companies do what they do best.[21] Just like it is no longer necessary for manufacturers to be in

---

[18] *Ibid*.

[19] In this sense, power is said to be a "commodity".

[20] Nicholas G Carr, *Does IT matter?: information technology and the corrosion of competitive advantage* (Harvard Business Press, 2004).

[21] A freqiently touted advantage is the ability to eliminate IT concerns and focus on core business activities. For example, see, Penny Crossman, "Fieldpoint Private Bank Turns to Cloud Computing for CRM and Beyond", *InformationWeek* (13 July 2010), online: <http://www.informationweek.com/news/225702942> (The bank's chief administrative officer explained; "One of my goals is to put as much of our technology in the cloud as possible.... I'm a big believer in aligning expense to revenue and keeping my capital expense down to a minimum, so cloud-based solutions make sense. I also believe that our firm needs to focus on its core competency, which is not technology but providing a high level of service to our members. As a result I'm not interested in maintaining a large IT staff or huge IT infrastructure, and believe we should focus on best-in-class IT services."

the power generating business, it is also no longer necessary for most companies to be in the IT business. Salesforce, one of the most successful cloud vendors, epitomizes the new ethos with its "no software" logo.[22] Even companies that are in some aspect of the software business can choose which parts to compete in, and rent the rest. Consequently;

> *Cloud computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it.*[23]

This has changed the startup equation, notably by lowering capital requirements and barriers to entry.[24] Facebook illustrates this point. Although the company's product is itself a cloud service, Facebook was for the first years of its existence also a cloud customer, renting computing power from others. In an evolution common to the most successful Internet companies, Facebook broke ground on its own data center in Oregon, in 2010.

> *Initially, **as most Internet startups do**, we leased data center space alongside other companies in the same building. As our user base continued to grow and we developed Facebook into a much richer service, we reached the point where it was more efficient to lease entire buildings on our own. We are now ready to build our own.*[25]

Facebook's remarkable rise from its founding in 2003 to the more than 8 million worldwide users it claims as of 2012 is a harbinger of the world to come; the freedom not to focus on infrastructure and the overhead it entails will help promote innovation on an unprecedented

---

[22] "Salesforce", (9 April 2012), online: *Salesforce* <http://www.salesforce.com/>.

[23] Armbrust et al, *supra* note 8 at 3.

[24] Jonathan Boutelle, "How Cloud Computing Impacts the Cash Needs of Startups", (16 August 2010), online: *GigaOM* <http://gigaom.com/cloud/how-computing-impacts-the-cash-needs-of-startups/>.

[25] Jonathan Heiliger, "Breaking Ground on Our First Custom Data Center", (21 January 2010), online: *Facebook* <http://blog.facebook.com/blog.php?post=262655797130>.

scale.[26] Cloud computing is revolutionising the way the world works. Functions that were once performed on individual computers are now performed in giant data centers, often those of one of a handful of dominant companies, such as Amazon or Google. Human intelligence, memory, problem solving and more has been outsourced first to our own computers and now, increasingly to cloud providers.

[26] See, for example, Vivek Kundra, *The Shift to Cloud Computing* (Washington, DC, 2010, online: < http://www.cio.gov/documents/Vivek-Kundra-World-Economic-Forum-Remarks.pdf>.

## 2.5 Bandwidth

Although increased connectivity has helped make the cloud possible, communications speed, bandwidth, stubbornly remains a factor. Despite the 1990s bubble for "infinite bandwidth" connection speeds vary widely by geographic location. In an extreme example, a South African publicity stunt pitted Winston, a carrier pigeon, against Telkom, the country's dominant Internet provider. Winston took 4 GB (in a thumb drive taped to his leg) 60 miles in about two hours, at which point only four percent of the data had made the trip[27]. In North America, as of 2009 it was still faster (hours) to overnight ship 10 TB of data rather than upload it at a speed of 20 mbps, which would be considered a good speed in North America .[28] A group of authors note that, assuming a 20 Mbs transfer rate, it would take 45 days to transfer 10 terrabytes of data; the same data could be sent on disks in an overnight package.[29] Generally, however, it is cheaper to ship data than power, and data center providers will locate in low-cost areas.[30] Amazon recommends and uses FedEx to ship large amounts of data, "bypassing the Internet".[31] The importance, and variability, of Internet connections also belies the myth that the Internet is making geography irrelevant. Places with high-speed Internet availability – typically cities or other areas that happen to be near the Internet "backbone" make much better locations for data centers than other areas and such real estate can command premium prices.[32] Microsoft's

---

[27] "SA pigeon 'faster than broadband'", *BBC Online* (10 September 2009), online: <http://news.bbc.co.uk/2/hi/8248056.stm>.

[28] The average U.S. "broadband" speed in 2009 was closer to 5 mbps and remains at about that level. At the time South Korea has the world's fastest speeds, averaging over 20 mbps. Better-connected locations in the United States can top 20 mbps. Other markets (mostly rural) in the United States can experience speeds in the tenths or hundredths of mbps.

[29] Armbrust et al, *supra* note 8.

[30] *Ibid* ("Physics tells us it's easier to ship photons than electrons; that is, it's cheaper to ship data over fiber optic cables than to ship electricity over high-voltage transmission lines.").

[31] "Amazon cloud uses FedEx instead of the Internet to ship data", *Network World* (10 June 2010), online: <http://www.networkworld.com/news/2010/061010-amazon-cloud-fedex.html>; For other examples, some humourous, see; Wikipedia contributors, *Sneakernet* (Wikimedia Foundation, Inc., 2012).

[32] Paul Jaeger et al, "Where is the cloud? Geography, economics, environment and jurisdiction in cloud computing", (May 2009), online: *First Monday* <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171>.

choice of its Virginia location for the new data center specifically noted the proximity to an existing government data center as a factor in favour of the chosen location.[33] Such concerns are not unusual. Although the amount of connectivity – bandwidth – available has continued to rise steadily, making more and more bandwidth-hungry applications and services possible, it remains "slow and expensive to ship data."[34]

Big institutions, such as businesses or universities can provide their own Internet connections, generally far exceeding what is available to consumers. However, most consumers and smaller to medium sized businesses are dependent on commercial last-mile intermediaries. The speed available may impact the viability of various cloud offerings. At a certain level of efficiency it becomes more economical to move data than to move electricity or physical disks. Netflix provides an example. The company started shipping DVDs by mail. However, sometime in the last few years it became more economical to ship bits than discs. Sometime in 2010, streaming Netflix rentals surpassed movies by mail in sales revenue. When Netflix launched in Canada in 2010, it skipped the postal model and operates there as a streaming only company.[35] Google – which obviously has an interest in promoting online activity – hopes to showcase the possibilities in a world where bandwidth is almost limitless by today's standards when it wires Kansas City, Kansas with 1 tbps fiber optic cable.[36]

---

[33] Miller, *supra* note 9.

[34] Ed Dumbill, "Big data in the cloud", *O'Reilly Radar* (22 February 2012), online: <http://radar.oreilly.com/2012/02/big-data-in-the-cloud-microsoft-amazon-google.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+oreilly%2Fradar%2Fatom+%28O%27Reilly+Radar%29>.

[35] Wikipedia contributors, *Netflix* (Wikimedia Foundation, Inc., 2012) online: <http://en.wikipedia.org/wiki/Netflix#cite_note-canada-119>.

[36] "Google Fiber & Kansas City",, online: <http://www.google.com/fiber/kansascity/about.html> Google explained; "To put this all in context, Google Fiber will deliver 1 gigabit Internet speeds – that's roughly 20,000 times faster than dial-up and more than 100 times faster than a typical broadband connection! Over the past decade, the jump from dial-up to broadband has led to streaming online video, digital music sales, video conferencing over the web, and countless other innovations that have transformed communication and commerce. We can't wait to see what new innovations will emerge as Kansas City moves from traditional broadband to ultra high-speed fiber optic connections."

## 3. THE CLOUD'S FOOTPRINT

### 3.1 Concentration and economies of scale

The Internet, or "the cloud" can seem an amorphous, ethereal phenomenon; where does our query go when we send a query to Google? Where is your Facebook profile stored? In reality, the Internet – or at least any specific part of it – has a specific location, and more and more frequently this is a data center. Facebook stores North American data in two giant data centers, one in North Carolina and one in Prineville, Oregon.[37] Google has several – at least six in the United States and one each in Belgium and Finland.[38] These data centers may be essential to the cloud model itself, even if the exact scope of the economies of scale benefit is debated.[39] When the Internet started as a network of academics and researchers, its component data was stored primarily on the computers of its users.[40] It is still possible to have a server in the home or business office, storing one's own data and serving up one's own web pages. However, it is becoming increasingly the norm to rent rather than buy or build "rack space." Having an unlimited amount of computing power available on demand and without capital expense may be an even more important benefit.[41]

---

[37] Heiliger, *supra* note 25.

[38] "Google Data Center Locations", online: *Google* <http://www.Google.com/about/datacenters/locations/index.html>.

[39] ("[The] construction and operation of extremely large-scale, commodity-computer datacenters at low-cost locations was the key necessary enabler of Cloud Computing, for they uncovered the factors of 5 to 7 decrease in cost of electricity, network bandwidth, operations, software, and hardware available at these very large economies of scale.")Armbrust et al, *supra* note 8;
But see, Christopher S Yoo, *Cloud Computing: Architectural and Policy Implications* (Philadelphia: University of Pennsylvania, 2011) Prof. Yoo questions the economies of scale argument; "A closer analysis reveals that some of the considerations that are often cited as supporting cloud computing (such as scale economies and converting capital expenditures into operating expenditures) may be less compelling than they initially seem. Instead, the primary advantages are the result from the benefits of aggregating demand".

[40] For a detailed history of the development of the World Wide Web, see Tim Berners-Lee & Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor* (Paw Prints, 2008).

[41] For example, "[Users] need not be concerned about overprovisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or underprovisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT." Armbrust et al, *supra* note 8 at 3.

### 3.2 Data centers

The world is experiencing a data center building boom.[42] Data centers have been hosted in converted and repurposed buildings, such as defunct factories[43] or unused skyscrapers.[44] However, increasingly as the "home" of the Internet, data centers are a new type of architecture. The "Terremark Building" – officially the NAP ("Network Access Point") of the Americas –offers an example. Most Internet traffic in to and out of South and Central America passes through a 750,000 square foot building in downtown Miami owned by Terremark, a Verizon subsidiary. Terremark advertises the building is designed to withstand a category 5 hurricane and outside the FEMA-designated 500 year floodplain. Just in case, the equipment is on the second floor, 32 feet above sea level. Seven-inch thick steel doors and 24 hour security protect against human intrusion. The building has multiple power sources and multiple connections to the Internet.[45]

Other data centers have similarly heavy footprints and elaborate and redundant systems. Apple's giant new Maiden, North Carolina data center, is now visible on Google maps satellite view.[46] In a move rumored to be at Apple's request, the site was obscured from view until just

---

[42] Anton Troianovski, "Storage Wars: Web Growth Sparks Data-Center Boom", *Wall Street Journal* (7 July 2011), online: <http://online.wsj.com/article/SB10001424052702303763404576417531646400002.html>.

[43] See, for example, Maija Palmer, "Where the Internet Lives", *Financial Times* (17 February 2009), online: <http://www.ft.com/cms/s/0/878ac3ba-d31b-11de-af63-00144feabdc0.html>.

[44] Julie Satow, "In Former New York Telephone Tower, Sabey Corp. Plans Data Centers", *The New York Times* (14 February 2012), online: <http://www.nytimes.com/2012/02/15/realestate/commercial/in-former-new-york-telephone-tower-sabey-corp-plans-data-centers.html>.

[45] "NAP of the Americas, South Florida Data Center, Tier IV Facility, Terremark", online: *Terremark* <http://www.terremark.com/technology-platform/nap-of-the-americas.aspx>.

[46] http://www.Google.com/maps?q=U.S.+Route+321+and+Startown+Road,+maiden,+nc&hl=en&ll=35.587876,-81.26117&spn=0.009266,0.024548&sll=45.50867,-73.553992&sspn=0.511036,1.571045&vpsrc=6&hnear=Startown+Rd+%26+U.S.+321,+Maiden,+Catawba,+North+Carolina+28650&t=h&z=16

before the launch of Apple's iCloud, which will be based there.[47] Twitter's new custom center in Utah has three connections to the Internet. Visa has elaborate security, including a moat, for the data center from which its network is run. The company will only say that its secret location is somewhere on the East Coast.[48] The terrestrial homes of the Internet are also power hungry. Facebook drew heavy criticism for its choice of Prineville, Oregon for its first data center because the area gets its power from coal. The company's North Carolina data center runs on a mix of coal and nuclear – and an estimated 3.6 percent renewable energy.[49] Thus it can be said that, at least in the U.S., Facebook runs mostly on coal with some nuclear power. Due to the heavy and increasing amounts of power consumed by the data center industry, building more efficient centers has become a topic of concern as well.[50]

### 3.2.1 In pursuit of the greenest location

Much of the power consumption of data centers is related to cooling as the thousands of computers inside produce heat as they run. Companies are thus prompted to locate in places where either power is cheap or less cooling is needed. One data center under Stockholm heats homes with the excess power. Ireland's relatively cool climate was one factor of many in Microsoft's decision to build there.[51] Facebook announced in October 2011 that it would soon start building a European data center near the edge of the Arctic Circle in Sweden. The center

[47] "Apple's invisible data center finally appears on Google Earth", *Technolog*, online: <http://www.technolog.msnbc.msn.com/technology/technolog/apples-invisible-data-center-finally-appears-google-earth-123066>; "Apple's North Carolina iCloud Data Center Finally Appears on Google Maps", (1 June 2011), online: <http://www.huffingtonpost.com/2011/06/01/apple-data-center_n_869596.html>.

[48] Michael Fitzgerald, "How Visa Protects Your Data", *Fast Company*, online: <http://www.fastcompany.com/magazine/160/visa-secret-security-center>.

[49] Miguel Helft, "Facebook Chooses North Carolina for New Data Center", *New York Times* (11 November 2010), online: <http://bits.blogs.nytimes.com/2010/11/11/facebook-chooses-north-carolina-for-new-data-center/>.

[50] "Greenpeace scorecard documents greener enterprise offerings", *Computerworld* (8 February 2012), online: <http://www.computerworld.com/s/article/9224063/Greenpeace_scorecard_documents_greener_enterprise_offerings>.

[51] Palmer, *supra* note 43.

will need much less cooling than the North Carolina location and will be powered by hydroelectric power.[52]

Cloud providers are also turning to models that move tasks around based on changing conditions. An example is provided by Google's newest "chiller-less" data center in St. Ghislain, Belgium. The center will use no energy for cooling, but will instead simply shut down and send its tasks elsewhere when the temperature gets too high. Google estimates that, given the local climate, it will need to turn off about seven days a year.[53] Technologists sometimes employ models based on "following the moon" or "following the sun."[54] Storage and computing are frequently most efficient at night when either less cooling is needed, electricity is cheaper, or both. Conversely, in a solar powered model the most desirable locations at any time will be where the sun is giving the most free energy. Cloud locations must be chosen as a complete package. For example, Iceland is in many respects an ideal location, but its seismic activity has caused concern among some would-be clients.[55]

---

[52] Leslie Horn, "Facebook Picks Sweden For First Data Center Outside U.S.", *PC Mag* (27 October 2011), online: <http://www.pcmag.com/article2/0,2817,2395378,00.asp> The Swedish choice is not without controversy Greenpeace, which has criticized Facebook for its reliance on coal and nuclear in the US, said it would like to know more facts before commenting on the Arctic site Privacy advocates may not be thrilled by the choice of Sweden; the country has a law allowing warrantless intercept of cross-border Internet communications Google has previously said the law categorically eliminated Sweden as a possible data center location for it; Ann Leach, "Facebook's Swedish data center will be subject to Snoop Law • The Register", *The Register* (31 October 2011), online: <http://www.theregister.co.uk/2011/10/31/facebook_swedish_data_center_privacy_law/>.

[53] "Google's Chiller-less Data Center » Data Center Knowledge", *Data Center Knowledge*, online: <http://www.datacenterknowledge.com/archives/2009/07/15/googles-chiller-less-data-center/>.

[54] *Cloud Computing* (Computer and Communications Industry Association, 2009), online: <http://www.ccianet.org/CCIA/files/ccLibraryFiles/Filename/000000000151/Cloud_Computing.pdf>.

[55] Jan Ziervogel, "The Natural Location for a Data Center", (2012), online: <http://www.greendataisland.com/Volcanoes.html>.

### 3.3 Jurisdiction indifference?

Many factors go into choosing a data center location; from a technical perspective, some argue it would be best if the law could just get out of the way.[56] Important values, including business efficiency and reducing environmental impact could be better served if technologists could choose data center locations based purely on factors such as cost of power, proximity to markets, climate and cooling costs, availability of skilled labour, and similar factors. This type of jurisdiction indifference is perfectly reasonable. Later sections of this thesis will expose how jurisdiction indifference is however not a reality. Prime examples are laws that prohibit the export of data outside a given jurisdiction.

#### 3.3.1 Two types of jurisdiction indifference

"Jurisdiction indifference" would be possible in at least two ways. One could focus on the location of end-users. Cloud computing should not be neutral as to the jurisdiction of users, at least not while laws vary so much by country. For example, if the United States and the EU continue to provide such different levels of privacy and consumer protection it must remain relevant whether a user is in the United States or Europe. However, jurisdiction indifference could also mean neutrality as to the location of data centers. A provider such as Google should be able to send its computing tasks wherever they can be performed most efficiently. Unless and until the nations of the world converge on a compatible legal regime jurisdiction indifference as to end users is undesirable. Jurisdiction neutrality as to data centers should still be promoted. At stake more than just the profit margins of a few companies but also global concerns, such as the dependability and interoperability of the global Internet and how often, in how many places, and how efficiently data centers must be built and maintained. This split nature of jurisdictional concerns, between the location of infrastructure and the locations of clients, is an important characteristic of cloud computing.

[56] This was the theme of a presentation by Prof. Anupam Chander in 2011 at the University of Toronto Cloud Law conference Anupam Chander, *Who Shall Govern the Cloud?* (University of Toronto Faculty of Law, 2011), online: <http://cloudlaw.ca/who-shall-govern-the-cloud/>.

## 4. MODELS

### 4.1 Business efficiency

Generally, cloud computing will often be cheaper because cloud providers can utilize economies of scale to secure everything from hardware to service more cheaply.[57] Business can also avoid the under-and over-provisioning dangers mentioned above. Cloud provisioning enables a company to buy exactly how much computing power it needs, when it is needed. Time to come online is measured in minutes, rather than weeks to years for owned physical infrastructure. "Black Friday" 2008 provided a negative example of this. On the busiest shopping day of the year (the day immediately after American Thanksgiving), some retail websites experienced outages, whereas sites using Amazon's "elastic" services slowed down, but not unbearably.[58] Target recently suffered bad publicity or worse after its website crashed twice in six weeks. The company had recently left Amazon Web Services.[59] The cloud market stretches to companies of all sizes. The decision when it is preferable to build or rent computing power involves questions of scale, but also of a company's ability to estimate its peak loads, whether it wants to be in the information technology business, and the degree of customization needed, meaning the decision-making process will be different for every company. As noted above, many businesses also welcome the ability to focus on their core endeavours rather than IT projects that can otherwise be outsourced.

---

[57] Armbrust et al, *supra* note 8.

[58] "Black Friday traffic takes down Sears.com", *msnbccom*, online: <http://www.msnbc.msn.com/id/27957529/ns/technology_and_science-tech_and_gadgets/t/black-friday-traffic-takes-down-searscom/>; When websites are not "elastic" sudden spikes can cause outages. Unexpected spikes in usage can cause websites to crash. For example; MG Seigler, "The Web Collapses Under the Weight of Michael Jackson's Death", *Tech* (25 June 2009), online: <http://techcrunch.com/2009/06/25/the-web-collapses-under-the-weight-of-michael-jacksons-death/>.

[59] Stephanie Clifford, "Demand at Target For Fashion Line Crashes Web Site", *The New York Times* (13 September 2011), online: <http://www.nytimes.com/2011/09/14/business/demand-at-target-for-fashion-line-crashes-web-site.html>.

### 4.1.2 Government

One market segment with a reliably heavy demand is government, and governments have also become active cloud consumers. Britain is building a so-called "G-Cloud", a network of 12 "super data centers" to replace some 500 that the country currently uses.[60] Initial announcements were that the project is expected to save the treasury some 3.2 billion pounds sterling a year. The United States has announced a "cloud first" policy for government procurement. As former U.S. Chief Information Officer Vitek Kundra put it;

> "The United States Government is the world's largest purchaser of information technology, with an annual IT budget over $80 billion. Cloud computing provides a tremendous opportunity to both improve service delivery to citizens as well as lower the cost of Government operations. To accelerate the safe and secure adoption of cloud computing, we are driving standards for interoperability, data portability and security."[61]

Providers have moved to capture government markets, which have long been dependable customers for Microsoft desktop products. Amazon Web Services (AWS) has long served several municipal and state-government clients. The company can now meet U.S. Federal Information Security Management Act (FISMA) standards for many purposes and offers a government cloud "region" for the United States, enabling government agencies and contractors who are obligated to keep data within the United States to use its cloud services;

Previously, government agencies with data subject to compliance regulations such as the International Traffic in Arms Regulations (ITAR), which governs how organizations manage and store defense-related data, were unable to process and store data in the cloud that the federal government mandated be accessible only by US persons. Because AWS GovCloud is physically

---

[60] Miya Knights, "Memset signs up as provider for government cloud initiative", (27 September 2011), online: *Cloud Pro* <http://www.cloudpro.co.uk/cloud-essentials/public-cloud/1797/memset-signs-provider-government-cloud-initiative>.

[61] Kundra, *supra* note 26.

and logically accessible by US persons only, government agencies can now manage more heavily regulated data in AWS while remaining compliant with federal requirements.[62]

With the world's largest client at stake, the competition is sure to be tough. The U.S. Department of the Interior recently ended a lawsuit by Google alleging that it improperly excluded Google from consideration for a contract to consolidate the 13 communications systems it uses for 88,000 employees to a single system. Google had complained that the Interior Department unjustly specified that bids must be compliant with Microsoft's Business Productivity Office Suite. Google won an injunction stalling the contract in September 2011. Shortly after, Google moved to dismiss, citing the government's "agreement to update its market research and then conduct procurement in a manner that will not preclude plaintiffs from fairly competing."[63] The amount in controversy is small compared to the potential government cloud market. However, it is possible it could foretell a government-wide move away from a preference for Microsoft.

American dominance of available providers has caused controversy related to adoption outside the United States. Part of the concern pertains to the use of technology or companies based elsewhere – often the United States. The Danish City of Odense received an opinion from that country's data protection agency that it cannot use Google Apps, at least until it had conducted a fuller assessment of the risks involved.[64] A Dutch minister recently told the country's parliament the government was considering barring U.S. companies from bidding for government contracts, a position from which he has since retreated.[65] Canada has also

---

[62] "AWS GovCloud (US)", (2012), online: *Amazon Web Services* <http://aws.amazon.com/govcloud-us/>.

[63] *Motion to dismiss, in the matter of Google v. United States, in the United States Court of Federal Claims* (Google Inc., 2011).

[64] *Processing of sensitive personal data in a cloud solution* (Datatilsynet, 2011), online <http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/>.

[65] Loek Essers, "European Data Concerns Cloud Outlook for US Vendors", *PCWorld* (16 September 2011), online: <http://www.pcworld.com/businesscenter/article/240161/european_data_concerns_cloud_outlook_for_us_vendors.html>.

exhibited a reluctance to embrace the cloud for public sector uses. This includes statutes in British Columbia and Nova Scotia banning public sector use of foreign cloud providers. [66] This has had a notable impact in education, where Canadian universities lag proportionately very far behind their U.S. counterparts in cloud adoption.[67]

### 4.2 Consumer services

The consumer model for cloud computing is most often software as a service. Programs such as Gmail, Picasa, Evernote, Facebook, Microsoft's cloud productivity suite, and others all do various useful or entertaining things for consumers. All are also powered on a data center-driven model. This consumer cloud model usually involves selling advertising space, data, or both to third parties such as advertisers. Thus, Google (Gmail) reserves the right to read your mail in order to better target ads at users, and Facebook mines data to better target its ads.[68] Users – knowingly or not – trade their personal information for the services they use. In the words of a popular saying, "if you're not paying for the product, you are the product." There is a massive market for personal data in the United States that has existed since before the Internet. For example, Choicepoint, one of a few big data aggregators, has 19 billion records on

---

[66] David TS Fraser, "Canadian Privacy Law Blog: Cloud Computing and Privacy FAQ", (18 April 2011), online: *Canadian Privacy Law Blog* <http://blog.privacylawyer.ca/2011/04/cloud-computing-and-privacy-faq.html>; Fred H Cate, *Provincial Canadian Geogrpahical Restrictions on Personal Data in the Public Sector* (Washington, DC: The Center for Information Policy Leadership, 2008).

[67] Zack Whittaker, "Why is Canada reluctant to adopt cloud computing?", *ZDNet* (15 June 2010), online: <http://www.zdnet.com/blog/igeneration/why-is-canada-reluctant-to-adopt-cloud-computing/5314>; Jay Black, "Don't Cloud SFU Data", (3 February 2012), online: *Jay Black's CIO Blog, Simon Fraser University* <http://www.sfu.ca/itservices/about/depts/cio/cioblog/2012/02/dont_cloud_sfu_data.html> (Simon Fraser University's Chief Information Officer discusses the practical implications for his institution).

[68] "Google Terms of Service – Policies & Principles", (March 2012), online: *Google* <http://www.google.com/intl/en/policies/terms/> See, "11. Content License from You"; *Registration Statement on Form S-1, filed with United States Seccurities and Exchange Commission* (Facebook, 2012), online <http://sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm>. Note numerous references to using customer data to target ads. For example, "Advertisers can specify that we show their ads to a subset of our users based on demographic factors such as age, location, gender, education, work history, and specific interests that they have chosen to share with us on Facebook or by using the Like button around the web or on mobile devices. We allow advertisers to select relevant and appropriate audiences for their ads, ranging from millions of users in the case of global brands to hundreds of users in the case of smaller, local businesses. We believe that users have a better experience when ads are effectively tailored to them." (at page 76). .

Americans.[69] This model is most prevalent in the United States, at least in part because of the relative lack of restrictions on the use of personal data there.[70] The Internet and the ensuing vogue for data driven business models has led to speculation personal data may be the next bubble market. New York *Times* tech writer Quentin Hardy seemed to think the idea had gone too far when he heard a suggestion that credit card companies should forego their standard three percent fee and make their money instead through the aggregation of data.[71] The free model is often coupled with a "freemium" model in which a for-cost "premium" model exists beside an advertising-supported free model. Evernote offers a free service and also an improved service for which it charges. In addition to gmail, Google also offers Google mail through Google apps. The company does not reserve the right to read mail sent on the paid version.[72] Some consumer cloud services, such as Facebook, remain purely advertising-supported without a premium, ad-free version.

Cloud offerings can also be used as value-added enticements to use other services. Apple recently made a splash in the cloud services market with the announcement of its iCloud to replace the failed Mac.com and Mobile Me services.[73] Apple will allow users to store photos, music, videos, and more on through iCloud, making use of its own North Carolina data center. Users will receive 5 gigabytes of free storage, but items purchased through iTunes will not count toward total. The advantage will be that users will be able to access their music and data straight from the cloud, anywhere. The fact that iTunes purchases will not count toward the total might encourage users to buy more music from iTunes. However, for a fee users will be

---

[69] Marcy E Peek, "Beyond Contract: Utilizing Restitution to Reach Shadow Offenders and Safeguard Information Privacy" in Anupam Chander, Lauren Gelman & Margaret Jane Radin, eds, *Securing Privacy in the Internet Age* (Stanford: Stanford University Press, 2008); See also, Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (Yale University Press, 2012).

[70] For in depth descriptions of the advertising and targeting uses of personal data, see; Turow, *supra* note 69.

[71] Quentin Hardy, "The Big Business of 'Big Data' - NYTimes.com", *New York Times* (24 October 2011), online: <http://bits.blogs.nytimes.com/2011/10/24/big-data/>.

[72] See note 68.

[73] For a rather humourous account of the failure of Mobile Me, see; Joe Fay, "MobileMe drove Steve Jobs to foul-mouthed fury", *The Register* (9 May 2011), online: <http://www.theregister.co.uk/2011/05/09/jobs_swear/>.

able to store any more music that is in their iTunes libraries. Amazon and Google had also been working on their own cloud "music locker" type platforms.

### 4.2.1 The prevalence of Software as a Service offerings

Consumer products are typically ready-to-use SaaS (software as a service), offerings. However, the line between small business and personal use is not always clear. For example, an engineer at the Washington Post used Amazon EC2 to re-organize and present 17,481 pages of Hilary Clinton's files in nine hours.[74] All one needs to rent "instances" of computing power from Amazon is a credit card. Lively ecosystems also exist for app development built on top of Apple and Android platforms.[75] This activity includes elements of hobby but also commerce. Developers produce apps for fun, profit, to get noticed in the job market. However, as IaaS renting is rather unstructured, it would be of little use to anyone without considerable tech savvy.

Google Apps and Amazon Web Services offer IaaS and PaaS and market to small businesses but could also be used by individuals[76]. Nor is there a clear line between business and consumer users of the cloud. Many businesses, perhaps all but the biggest make use of cloud services offered on a take-it-or-leave it, purchase cloud services on an adhesion-contract basis. A survey from the cloud law project at Queen Mary University London illustrates the large number of such users.[77] Such contracts overwhelmingly favour providers, including by disclaiming warranties or consumer protections, or dictating choice of law or forum favourable to the provider. This underscores the fact that whatever non-waivable consumer protection law exists may effectively provide the only protection available to consumers. Many small businesses not

[74] Armbrust et al, *supra* note 8 at 9.

[75] "iOS Dev Center", (2012), online: *Apple Developer* <http://developer.apple.com/devcenter/ios/index.action>.

[76] note 12; note 12.

[77] Simon Bradshaw, Christopher Millard & Ian Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services* (London: Queen Mary University of London, School of Law, 2010) See table 1.

receiving legal protections intended for consumers also stand as consumers relative to cloud providers.

## 5. LEGAL THREATS TO A GLOBAL CLOUD

### 5.1 Jurisdictional overlap and conflict

Cloud users and providers face an overlapping set of considerations and risks related to data protection, jurisdiction risk, and privacy law compliance.[78] Litigation and "e-discovery" pose additional problems. Common law legal systems, especially American courts are known for the demands of their pre-trial discovery processes. American courts, in particular, allow for wide open discovery of "any matter relevant to the subject matter involved in the action."[79] This can sometimes conflict with European laws, particularly either blocking statutes or legislation intended to protect personal privacy. As an important EU advisory body has noted; "There is a tension between the disclosure obligations under US litigation or regulatory rules and the application of the data protection requirements of the EU."[80] Many nations have enacted so-called blocking statutes that either forbid or severely limit the ways in which local information can be used in foreign litigation. Although cases are decided on an individual basis, U.S. courts generally reserve the right to order discovery and production of documents (including electronic documents) regardless of legislation elsewhere.[81] A 2008 case saw a French lawyer fined 10,000 Euros for assisting in American e-discovery.[82] The French lawyer was fined under the French blocking statute.[83] Generally, U.S. courts are not impressed by foreign blocking statutes and will order parties to comply regardless of the trouble it could cause them overseas.[84]

---

[78] For example, see, Karin Retzer & Michael Miller, "Mind the Gap: U.S. Discovery Demands versus EU Data Protection", *BNA Privacy and Security Law Report* (13 June 2011), online: <http://www.mofo.com/files/Uploads/Images/110601-US-Discovery-Demands-versus-EU-Data-Protection.pdf>.

[79] *U.S. Federal Rule of Civil Procedure 26(b)(1)*.

[80] *Working Document 1/2009 on pre-trial discovery for cross border civil litigation* (Brussels: Article 29 Working Party).

[81] See, *Societe Nationale Industrielle Aerospatiale v. District Ct. for the S. Dist. of Iowa* (1987), 482 1987 US 522.

[82] Marc Gottridge & Thomas Rouheete, "France puts some muscle behind its blocking statute", *New York Law Journal* (29 April 2008), online: <http://www.hoganlovells.com/files/Publication/ed20ea51-6c49-4798-bd10-54c6f58f51b5/Presentation/PublicationAttachment/194fc242-489a-4db5-8ba1-a82bf053cdcd/France_Puts_Some_Muscle_Behind_Its_Blocking_Statute_29_04_08.pdf>.

[83] *Law No. 80-538 of July 16, 1980*, 16 July 1980 [*Law No. 80-538 of July 16, 1980*].

[84] *Gucci America, Inc v Curveal*, 09 Civ 8458. (S.D.N.Y. 2010)

### 5.1.1 Privacy regulations

In addition to blocking statutes, European privacy laws can also be incompatible with American-style laws and procedure. Incompatibility between systems can lead to dangers of compliance risks when organizations with a presence in two jurisdictions are faced with differing rules. Europe has protected any information about identifiable individuals under an E.U.-wide directive that is implemented slightly differently in each member country.[85] In the United States, certain classes of data, such as health information (HIPAA) are protected. In other cases, Americans may generally be accustomed to an environment in which it is acceptable to read employee emails sent during work hours or from work computers, especially if the employee is warned.[86] Such surveillance is typically impermissible in Europe. In 2001, the highest court of appeals in France rules that Nikon had violated the privacy rights of an employee by examining emails in his company account market "personal." The investigation revealed that he had been doing work for personal benefit on company time.[87] A French hotline set up for the French subsidiary of McDonalds to comply with the American Sarbanes-Oxley Act ("SOX") was found to violate French data protection laws.[88] Outright restrictions on cross-border transfers or misunderstandings based on lack of familiarity with foreign regulatory regimes can lead to costly problems for those using or designing cloud systems.

## 5.2 Fragmentation

Much attention has been paid to the fragmented state of regulations concerning data. European Union Digital Agenda Commissioner Neely Kroes has been promoting greater

[85] *Data Protection Directive*, 1995 [*95/46/EC*].

[86] For ex. see; *Muick v. Glenayre Electronics* (2002), 280 2002 F 3d 741.

[87] Doreen Cavajal, "Vigilance: Where to set limits?", *New York Times* (21 April 2004), online: <http://www.nytimes.com/2004/04/21/business/worldbusiness/21iht-workcol21_ed3_.html>.

[88] Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part 1)" (2010) 18:2 IJLIT 176.

integration of privacy regulations to better institute a "digital single market", arguing that the current patchwork slows economic growth.[89] Microsoft General Counsel Brad Smith has been making a similar case throughout Europe.[90] Even if laws were evenly applied throughout Europe, compliance with differing approaches to data and security worldwide would make worldwide compliance difficult. This has been noted at the highest levels of the EU, for example in the proposal to replace the Data Protection Directive with an EU-wide regulation.[91]

### 5.2.1 Canadian limitations

British Columbia and Nova Scotia strictly limit the use of foreign cloud providers by public bodies, including universities. Legislation in Alberta provides for punishment for providers who divulge information under court orders without jurisdiction in Alberta. The Privacy Commissioner of Canada has opined that the Canadian federal regulation, PIPEDA, does not prohibit outsourcing to the United States or elsewhere.[92] However, would-be users of outsourced cloud services are reminded that they are still responsible for the safety of data, and are also instructed to inform their users of the outsourcing;

> *A company in Canada that outsources personal information processing to a company that operates in another country should notify its customers that the information may be available to the government of that country or its agencies under a lawful order made in that country*.[93]

---

[89] Neely Kroes, *EUROPA - Press Releases - Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Ending fragmentation of the Digital Single Market Business For New Europe event London, 7 February 2011* (London, 2011).

[90] Brad Smith, *Remarks by Brad Smith, General Counsel and Senior Vice President, Legal and Corporate Affairs* (National Assembly, Paris, 2011) online, <http://www.microsoft.com/Presspass/exec/bradsmith/01-24-11FNA.mspx>.

[91] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Brussels: European Commission, 2012).

[92] Jennifer Stoddard, "Commissioner's Findings - PIPEDA Case Summary #394: Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers (August 7, 2008)", (2008), online: <http://www.priv.gc.ca/cf-dc/2008/394_20080807_e.cfm>.

[93] *Ibid*.

Such considerations can make for practical difficulties in deploying foreign-based cloud services anywhere in Canada, as when Lakehead University met with stiff faculty resistance to its plans to adopt Google-based services.[94] Measures that limit the use of U.S.-based cloud services do potentially impose real costs as they limit the number of options available to Canadian users. It is unlikely that homegrown solutions will soon be able to rival the options available in the U.S., with ten times as many consumers as Canada and also the world's foremost tech companies. Outlawing outsourcing outside of Canada can have serious cost implications, especially given the relatively small number of providers based in the Canadian market. For example, Universities in British Columbia and Nova Scotia cannot use U.S.-based services such as the plagiarism checker Turnitin.[95]

### 5.2.2 Extreme fragmentation – authoritarian regimes

Whatever the inconveniences of establishing cloud networks in countries with differences such as between the United States and Europe or Canada the most extreme examples of fragmentation are seen in authoritarian regimes, which are creating their own local Internets with limited connectivity to the outside world. China has aggressively moved to create a uniquely Chinese version of the Internet, controlling traffic in through the famous "great firewall", and possibly now also out through new privacy regulations. Several cloud giants, such as Facebook and Twitter do not operate in China. The market is instead served by local champions providing similar, but uniquely Chinese alternatives. Facebook is banned altogether. After years of difficult relations with the mainland Chinese government, Google moved its operations to Hong Kong in 2010. Google and business users of Google Apps have from time to

[94] Phillip Todd, "Switch to Google e-mail saves resources, raises privacy concerns", *University Affairs* (10 March 2008), online: <http://www.universityaffairs.ca/switch-to-Google-email-saves-resources-raises-privacy-concerns.aspx>.

[95] Katelyn E Neily, "Orato: UBC Student Data Illegally Stored in US BC's FIPPA Law Bans Turitin Plagiarism Check", (18 March 2012), online: *Orato* <http://www.orato.com/tech-games/ubc-student-data-illegally-stored-us>.

time in China as well.[96] China has possibly also co-opted privacy and data protection to the service of creating the largely separate Chinese Internet.

> *With data transfer restrictions and the hurdles which foreign companies must overcome to do business in China, we may see growth in local providers providing cloud services to onshore customers with all data centers located in China*.[97]

China has aggressively moved to create a uniquely Chinese version of the Internet, controlling traffic in through the famous "great firewall", and possibly now also out through new privacy regulations. Several cloud giants are supplanted by local champions providing similar, but uniquely Chinese alternatives. For example, market leaders such as Facebook, Google, and Twitter are all supplanted by local champions in China. Facebook is banned altogether. After years of difficult relations with the mainland Chinese government, Google eventually moved its operations to Hong Kong in 2010. Google and business users of Google Apps have experienced difficulties from time to time in China as well.[98]

---

[96] *Official Google Enterprise Blog: An update for our customers on Google Apps and China* (2010) online, <http://googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html>; "Google: China is messing with Gmail - Google 24/7 - Fortune Tech", (2010), online: <http://tech.fortune.cnn.com/2011/03/21/google-china-is-messing-with-gmail/>.

[97] Anna Gamvros, "Hong Kong and China Taking Different Routes to the Cloud", *BNA International* (March 2011), online: <http://www.bnai.com/HongKongChinaCloud/default.aspx>.

[98] note 96; note 96.

## 6. RISKS

Of course, the perceived advantages of cloud computing are not without risk. Trusting one's data or computing to another person or company necessarily requires some amount of risk. One way to inspire trust is of course through laws. Ideally this could be done in a manner that would support reliability, safety, and trust without unduly burdening users or suppliers. In many respects, cloud computing can be considered safer than self-hosted computing. For example, physical security failures – physically breaking into a building or stealing a computer – are often the single point of failure for end-users. Cloud computing can do much to alleviate concerns based on physical threats, but can add new levels of threat. Additionally, cloud computing might seem dangerous because of the fact that it necessarily involves trusting information to a third party. Law can – and should – play a role in alleviating these risks. However, sometimes law has contributed to the risks.

Cloud computing risks range from systems failure to the possibility of nefarious actions by employees along the length of chain of service providers, to many other risks. Those mentioned here are those in which law plays the biggest role in alleviating or aggravating the problem.[99] According to widely cited report, cloud computing can provide security benefits in a number of ways, first of all including the benefits of economies of scale in providing protection. "[P]ut simply, all kinds of security measures are cheaper when implemented on a larger scale." Other benefits include standardized interfaces for controlling security measures and "rapid, smart scaling of resources".[100] Critical for many legal functions (including litigation e-discovery), cloud computing can also provide for more efficient "audit and evidence-

[99] For example, consider the risk of so-called "side channel attacks". This is the risk that one tenant could somehow use its access to a cloud provider's service to access data belonging to a fellow tenant. Although law could have an effect on such a risk, for example by increasing hacking penalties, the risk itself seems less inherently legal than others. More inherently legal risks include dangers such as increased compliance difficulties because of exposures to multiple legal systems or the prevalence of one-sided contracts favouring providers over consumers. See, Kim-Kwang Raymond Choo, *Cloud computing: Challenges and future directions* (Canberra: Australian Government, Australian Institute of Criminology, 2010) online, <http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx>.

[100] Daniel Catteddu & Giles Hogben, *Cloud Computing: Benefits, risks and recommendations for information security* (European Network and Information Security Agency, 2009) online, <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment>.

gathering".[101] Since cloud computing enables software to be centrally controlled, users are more likely to have efficient updates of software and default settings. Since physical infrastructure is concentrated, efficiencies can also be achieved in protecting that.[102]

### 6.1 Will the market address risks?

An important European report optimistically states that "security as a market differentiator" will provide a "strong driver for cloud providers to improve security practices." This may be debatable, at least for the small business and consumer markets. Experience seems to indicate that many providers do not invest the effort and cost to make their services secure, for example through https encryption, until they come under pressure to do so from outraged experts.[103] "There simply isn't sufficient market demand for these firms to allocate the considerable financial and engineering resources required to deploy encryption by default for all of their products."[104] Google illustrates; the company first did not offer https encryption, then offered it as an option that only relatively savvy users were likely to find, and finally made it a default setting. However, each change came only under considerable pressure not from the general marketplace, but from a group of relative Internet technical and legal heavyweights.

A study of some of the clauses found in consumer cloud computing contracts might bolster the idea that the market – to date – provides poor mechanisms to guarantee privacy, safety, and

---

[101] Christopher Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era" (2009) 8 J on Telecomm and High Tech L 359, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553&http://www.google.com/url?sa=t&source=web&cd=3&sqi=2&ved=0CCwQFjAC&url=http%3A%2F%2Fpapers.ssrn.com%2Fsol3%2FDelivery.cfm%2FSSRN_ID1656471_code636196.pdf%3Fabstractid%3D1421553%26mirid%3D1&rct=j&q=soghoian%20cloud%20market%20failure&ei=BUXuTfzHD8zAgQf3o7yUDw&usg=AFQjCNFwsUqzpHWL8S3OWBHisYE80gDS8w&sig2=IiejGHaeb_7j9uMISbQ2IQ>.

[102] This is a related to the idea that data stored in a central cloud computing nerve center might be more secure than data dispersed throughout numerous end-user computers. Of course, resource concentration can also be dangerous if the location where resources are concentrated turns out to be dangerous or is hit by a disaster, etc.

[103] Soghoian, *supra* note 101.

[104] *Ibid* at 380.

quality.[105] Consumers by the millions give away privacy rights, allowing services to scan their mail to offer targeted ads, or other data-mining purposes. Many consumer services offer very one-sided terms in the event of a dispute or the end of service.[106] Amazon Web Services asks users to take their own security precautions, such as backups or encryption. Some providers predominantly used for backup purposes disclaim their fitness for the purpose for which they are marketed. Other services do not promise any particular level of service, except perhaps "best efforts".[107]

Thus, at the consumer level, a combination of factors, perhaps including consumer apathy and opacity in contracts seems to indicate that presently, competition on security does not lead to improved offerings for consumers. Dropbox might present an even more extreme special case; the company clearly stated terms favorable to consumers – that it did not hold encryption keys to user data – but actually did not live up to them.[108] Many small to medium sized businesses also lack bargaining power against cloud providers.[109] The uneven balance of power between vendor and customer in such contracts, and the fact that they are typically favourable to the vendor increases the importance of non-waivable legal protections.

For organizations with some bargaining power the situation is better. Government subdivisions have been able to negotiate, for example, contracts limiting the geographic area in which their

---

[105] Bradshaw, Millard & Walden, *supra* note 77.

[106] *Ibid* For example, Google Docs, upon which many people and organizations rely, claims that files are subject to deletion at any time. Apple's MobileMe states that all information is deleted immediately upon termination of the user contract. The terms of service do not address any provision for what how to handle cases where a contract may have been terminated wrongfully. .

[107] *Ibid*.

[108] Ryan Singel, "Dropbox Lied to Users About Data Security, Complaint to FTC Alleges", *Wired* (13 May 2011), online: <http://www.wired.com/threatlevel/2011/05/dropbox-ftc/#more-26298>.

[109] See tables accompanying Bradshaw, Millard & Walden, *supra* note 77; Legal Cloud Computing Association, *Response to North Carolina State Bar Proposed 2011FEO6 - Legal Cloud Computing Association* (Legal Cloud Computing Association, 2011) (noting lack of effective ability for most lawyers to negotiate specific points in cloud contracts: "Larger companies, such as Google or Microsoft, are not going to negotiate with North Carolina lawyers on this point. Small companies will simply pull out of the North Carolina market altogether").

data may be stored.[110] Consumers may also have power in the aggregate. Prompted by market forces, Amazon now offers four geographic divisions of its cloud service coinciding with major regulatory regimes.[111] Depending on which one the customer chooses, Amazon is contractually obligated to keep data within that geographical area. Big customers are advised to negotiate many key provisions from cloud providers, including ownership of data, responsibilities in litigation and e-discovery, provisions that data is held in-trust or under duty of bailment, and guarantees of liquidated damages for data breach.[112]

### 6.2 Government requests

When government is seeking information, no cloud provider can guarantee users' complete protection; there are simply too many cases in which government will have the authority and the power to compel disclosure of account information, content, or both.[113] Cloud service providers can, however, differentiate themselves on how they handle requests for information, such as subpoenas. Twitter, for example, has a policy of notifying users of requests for their information unless they are prohibited from doing so.[114] The company has won praise for its

---

[110] Timothy Trappler, "If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues", *Educase Quarterly* (2010), online: <http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfItsintheCloudGetItonPaperClo/206532>(Noting limitations on data transfers, including those obtained by the city of Los Angeles) .

[111] The divisions are: U.S., U.S. California only, Europe (based in Ireland), and Asia (based in Singapore).

[112] David TS Fraser, *The Cloud Thing: Privacy and cloud computing* (Dalhousie U. Halifax, N.S., 2011) at 24(desirable cloud contracts for users); Nicole Convery, *Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud* (Department of Information Studies, Aberystwyth University, 2010)(advice for institutions negotiating cloud contracts).

[113] In many regulatory schemes, "content" is treated differently from "account" type information. For example, see; *Electronic Communications Privacy Act*, 1986, 27 USC 2701 et seq [*ECPA*] Note the differing treatment of "content" and "subscriber" information under the Stored Communications Act in the United States. Likewise, the "National Security Letters" authorized by the USA Patriot Act compel disclosure of account and billing information, rather than the content of communications. 27 USC § 2709. .

[114] "Twitter Help Center, Guidelines for Law Enforcement", (2012), online: *Twitter* <https://support.twitter.com/articles/41949-guidelines-for-law-enforcement>.

resistance of subpoenas related to Wikileaks and the Occupy Wall Street movement.[115] The move to store data within geographic zones was in part prompted by cloud providers' desire to offer services that met regulatory requirements, such as storing personal data within Europe or avoiding the reach of the U.S. Patriot Act. However, this tactic has been cast in doubt by the extraterritorial reach of many laws.

### 6.3 Vendor Lock-in

Cloud users also face the possibility of "vendor lock in", the inability to change providers at a reasonable cost.[116] This can be by design or by accident. Facebook provides an example. There is no way to move user data into and out of the service. To leave Facebook is to write off a potentially large sunk cost in terms of the social network one has built there. Facebook benefits from this each time it makes a controversial security or privacy setting change; Users may grumble, and a few may quit, but most stay. If Facebook used a common API or interface where users could pick up and leave – but bring their contacts with them – the equation might be different. Since 2007 Google has had a team known as the "Data Liberation Front" whose mission is to "make it easier to move data in and out" Google claims to do this "because we want our users to stay with us because they want to."[117] The proposed EU reforms, as currently written, would provide data subjects the right to "data portability", enforced by a guarantee that they would have the right to data about them in a "structured and commonly used electronic format."[118]

---

[115] "Twitter Ignored Request To Keep Subpoena Under Wraps [UPDATED]", *ReadWriteWeb* (27 December 2011), online: <http://www.readwriteweb.com/archives/twitter_ignored_request_to_keep_subpoena_under_wraps.php>.

[116] Lock in could also have further detrimental effects on the ability for market forces to exert positive forces for desirable outcomes such as security. If consumers cannot credibly threaten to change providers because the costs of doing so are too high, then providers will have little reason to offer improved service or security.

[117] "Data Liberation Front", (2012), online: *Google* <http://www.dataliberation.org/>(See FAQ section).

[118] European Commission, *supra* note 91 online, <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>.

Business also wants interoperability. Some of the biggest cloud spenders have devoted themselves to a multi-billion dollar campaign to force vendors into offering products that will work well together.[119] Government surely has a role to play in ensuring world cloud interoperability, and the decisions will not be easy.[120] European and American law and regulatory enforcement will probably dictate differing results.[121] Fostering growth through antitrust law is sure to present tough balancing acts for regulators worldwide.[122]

[119] Charles Babcock, "User Alliance Wants Cloud Interoperability", *InformationWeek* (8 June 2011), online: <http://www.informationweek.com/news/cloud-computing/infrastructure/230400015>.

[120] Ian Walden & Laise Da Correggio Luciano, "Ensuring Competition in the Clouds: The Role of Competition Law?" (2011) SSRN eLibrary, online: <http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1840547>.

[121] Jeremy D Feinstein, "Tying Up the Cloud: A Study in Antitrust Issues in Cloud Computing" in *Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing* (Reed Smith, 2010).

[122] *Cloud Legal Project response to European Commission Cloud Computing Consultation, Queen Mary, University of London* (London, 2011) online, <http://www.cloudlegal.ccls.qmul.ac.uk/Research/55027.html>.

## 7. NEED FOR REGULATION

Research suggests that markets alone are not sufficient to provide security and fairness to cloud users.[123] Numerous examples suggest that consumers do not read, do not understand, or do not care about the contents of cloud contracts. This was humourously illustrated in 2010 when UK gaming company Game Station included a clause in its click-through contracts online stating, "By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul."[124] Customers were even given a chance to opt-out of the "immortal soul clause" – and receive a valuable coupon instead; only 12 percent did so.

Researchers with the Queen Mary University Cloud Law Project paper surveyed common consumer cloud law contract provisions and raised concerns about the content of contracts of cloud services marketed at individuals and small-to-medium sized businesses. Of 31 contracts surveyed;

> [T]he majority of contracts favour the provider, in some cases to the extent of risking being unenforceable [under EU law], especially against consumers and small/medium sized enterprises (SMEs) under laws such as those implementing Council Directive 93/13/EEC on unfair terms in consumer contracts. Furthermore, cloud providers reserve the right to, and do, from time to time change their standard terms, seemingly without adequate or any notice to users, who are forced to attempt to compare the terms to see what the changes are (assuming they have saved a copy of the previous version(s)). Terms published online may or may not indicate their date of issue, and even if updated may not necessarily indicate on their face that they have been changed, let alone which terms have been changed and in what way."[125]

---

[123] Soghoian, *supra* note 101.

[124] Catherine Smith, "7,500 Online Shoppers Accidentally Sold Their Souls To Gamestation", *Huffington Post* (17 April 2010), online: <http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html> online, <http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html>.

[125] The response was drawing on data further described in; note 122; Bradshaw, Millard & Walden, *supra* note 77.

European consumers are much more likely than their American counterparts to enjoy protection from abusive contracts. Such protection can even extend to businesses.[126] In the United States, the most important line of protection comes from FTC enforcement against unfair competition practices. In the context of online consumer contracts, "unfair" means only deceptive. This was illustrated by the recent Dropbox case. Dropbox, a popular consumer application for storing, sharing, and syncing documents across devices, was alleged to have exaggerated claims about its security. The service claimed it had no access to user files because only the user held an encryption key. In reality, Dropbox did have access to the files, a difference that had implications for at least possible employee snooping or law enforcement access. Two Dropbox competitors made security claims similar to those of Dropbox but actually followed through, putting them at a competitive disadvantage.[127] Dropbox has since changed its explanation of the service. It could be said that the Dropbox case is an example of the system working; a company did something deceptive, got caught, suffered bad publicity, and changed its practice. This is consistent with the usual American approach. However, for this to work requires some amount of regulatory backstop, in this case from the FTC, which would have been empowered to pursue an investigation of Dropbox if the deceptive practice had continued.

### 7.1 Privacy policies

Privacy policies can be especially important for U.S. sites because they often lay out the only protections available to consumers. The proportion of U.S. websites that publicize privacy policies has increased markedly since the 1990s, largely driven by consumer awareness of the privacy risks involved in information sharing on the Internet. This consumer awareness has in turn been driven largely by data-breach notification laws, starting with California's in 2002.[128]

---

[126] *Kingsway Hall Hotel v Red Sky IT (Houslow)* [2010] EWHC 965 (TCC). The court noted the imbalance in sophistication between the IT company and the plaintiff.

[127] Singel, *supra* note 108.

[128] see Raymond T Nimmer, "Contracts, Markets, and Data Control" in *Securing Privacy in the Internet Age* (Stanford: Stanford University Press, 2008).

California's requirement for websites to have privacy policies – in place since 2003 – also requires any website targeting Californians to post a privacy policy, basically creating a de-facto national standard because national businesses cannot ignore California.[129] In one example, Google reluctantly affixed a privacy policy to its homepage despite its stated preference to keep the homepage as uncluttered as possible. An optimistic case for market-based solutions to security issues in the United States could be that if consumers can rely on the FTC to enforce promises under unfair competition law and data-breach notification laws to give companies an incentive to safeguard their information, then companies that make and uphold better promises will rise to the top.

[129] *Online Privacy Protection Act of 2003*, 2003, Cal Bus & Prof Code 22575-22579 [*Online Privacy Protection Act of 2003*] online, <http://leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579>.

## 8. U.S. LEGAL ENVIRONMENT

The United States is, effectively, the home of cloud computing. This is evident in both the dominance of U.S. cloud providers[130] and the amount of money invested in the cloud worldwide.[131] Prominent and characteristically American risks to the cloud computing business climate in the United States are the perceived danger of government surveillance (epitomized by fears about the Patriot Act[132]), costly discovery rules in civil cases, and uncertainty over the exact parameters of government access to data in criminal cases (as under the Electronic Communications Privacy Act).[133] Nevertheless, the overall outlook for cloud computing in the United States is as good as or better than anywhere else in the world. Particularly helpful in this are liberal rules regarding freedom of contract and recognition of consumer contracts and the lack of any universal data protection regime.

### 8.1 Freedom of Contract

Cloud providers in the United States can generally form contracts with consumers online with the expectation they will be enforceable in a court of law. Since the *Zeidenburg* decision, so-called "click-wrap" contracts have gained in popularity and are now the standard.[134] Non-negotiated contracts ("contracts of adhesion") are generally enforceable, at any rate to a much higher degree than in European countries. European consumers generally receive a higher degree of protection than American consumers.[135] Agreements between providers and consumers, including agreements to arbitrate or venue selection clauses, are generally

---

[130] O'Brien, *supra* note 2 (prevelance of U.S. providers).

[131] Craig Hanson, "Next World Capital", *New World Capital* (2012), online: <http://www.nextworldcap.com/newsletter/article.php?id=1>.

[132] *USA Patriot Act*, 1 February 2002 [*Patriot Act*] The USA PATRIOT Act, Public law 107-56, was not codified in one place, but was instead a set of changes to other laws found in the following titles of the United States Code; 8, 12, 15, 18, 20, 31, 42, 47, 49, 50; See, Charles Doyle, *The USA PATRIOT ACT: A Legal Analysis* (Washington, DC: Congressional Research Service, 2002).

[133] ECPA, *supra* note 113.

[134] *ProCD, Inc. v. Zeidenberg* (1996), 86 1996 F 3d 1447.

[135] See generally, Bradshaw, Millard & Walden, *supra* note 58.

enforceable.[136] American courts do place some limits on what contract terms will be enforced, but the limits are generally lax.[137]

### 8.2 Privacy

In Europe, the next biggest cloud market, privacy is considered a human right.[138] In the United States, free speech and the free flow of information has been given much greater protection. For example, the recent *IMS v. Sorrell* case overturning Vermont's law limiting the sale of prescription drug information to data mining companies (who use it to market drugs to physicians) did not place much emphasis on the privacy interests of the "anonymous" patients involved.[139] In fact, in the United States, a mere loss of personal data without more may not constitute actionable loss.[140] The United States Supreme Court held in 1977 that there is no

---

[136] Contrast to Europe where consumer protection legislation gives consumers the right to sue in the courts of their home country. (Hague Convention on Choice of Court Agreements, 2005 – Section II excludes contracts "to which a natural person acting primarily for personal, family or household purposes (a consumer) is a party" from the general rules permitting choice of forum agreements. *The Hague Convention of 20 June 2005 on Choice of Court Agreements* (2005), section (1)(a) online, <http://www.hcch.net/upload/conventions/txt37en.pdf>.

[137] *Bragg v. Linden Research, Inc.* (2007), 487 2007 F Supp 2d 593 The plaintiff sued the maker of the popular "Second Life" virtual world game, claiming that the mandatory arbitration clause was procedurally and substantively unfair. The trial court, applying California Law, held that a finding of unconscionability was supported by at least the following factors; lack of mutuality, excessive arbitration costs, venue in California, confidentiality agreement (gag order on plaintiffs), business reality – terms were excessive as to what was required to protect business. (Upheld on appeal to 3rd Circuit.) .

[138] *European Convention on Human Rights 8.1*, 1950 [*ECHR 8.1*].

[139] *Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) In Support of Appellee and Urging Affirmance, Sorrell v. IMS* (Electronic Information Privacy Center, 2009) arguing that "… in addition to the concerns expressed about the privacy of prescriber [doctor] data, there are also substantial concerns for the privacy of patient data. Further, the techniques for anonymity contemplated in the statute are not adequately enforced to safeguard these interests." online, <https://epic.org/privacy/ims_sorrell/epic_amicus.pdf>; Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines* (Brussels: Article 29 Working Party, 2008) Contrast to the EU Article 27 Working Party's concern for problems such as the "AOL case", where "Even though AOL had replaced the names of the users by a number, journalists found out these results could often be traced to individual users…" online, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf >.

[140] See, *In Re. JetBlue Privacy Litigation* 379 F. Supp. 2d 299 (E.D.N.Y. 2005). Despite express promise that various passenger data would not be shared with third parties, JetBlue sold a bulk set of data to the defense contractor Torch for use in a data-mining project. The court dismissed "[Plaintiffs] had no reason to expect that they would be compensated for the "value" of their personal information. In addition, there is absolutely no support for the proposition that the personal information of an individual JetBlue passenger had any value for which that passenger could have expected to be compensated."

"general constitutional right to privacy."[141] Nevertheless, the Court seemed to indicate that a theoretical right to informational privacy from the government may exist under the constitution;

> *We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed*.[142]

At the time of the decision above, the Privacy Act of 1974 already provided some statutory protections for the handling of information by private information by agencies of the federal government.[143] However, its protections do not extend to the states, although many have adopted their own privacy statutes regulating the way the states handle personal information. In a prescient concurrence, Justice Brennan expressed his awareness of what has now been labeled by some "the creep factor" of vast stores of information.[144]

> *What is more troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously, as the State argues, collection and storage of data by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. However, as the example of the Fourth Amendment shows, the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology*.[145]

---

[141] *Whalen v. Roe* (1977), 429 1977 US 589 at 608.

[142] Whalen v. Roe, *supra* note 141.

[143] *Privacy Act*, 5 USC § 552A [*Privacy Act of 1974*].

[144] Turow, *supra* note 69.

[145] Whalen v. Roe, *supra* note 141 at 607.

The checks on the information practices of the federal government remain statutory and not constitutional. By statute, U.S. federal agencies must have privacy policies in place.[146] A blanket prohibition on sharing states that; "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains…"[147] A number of exceptions permit most uses necessary to perform the vital functions of the government, such as law enforcement, Congressional investigations, statistics, and archives. There is no general expectation of privacy in information held by state governments that is widely available from many sources and often exposed in public.[148] In the words of one decision; "We seriously doubt that an individual has a constitutional right to privacy in information routinely shared with strangers."[149]

Nor will it generally be considered an invasion of privacy for companies to make use of information shared with them by their customers. [150] Companies are bound only by their own privacy promises. Even this enforcement will only be to the extent that the market or the FTC reacts. The 1974 Privacy Act was intended by some of its more enthusiastic supporters to be a "comprehensive" data protection regime in the European model.[151] Passage of such an act

[146] The privacy bill was co-sponsored by conservative Representative Barry Goldwater and liberal New York Representative Ed Koch (later mayor of New York City). Earlier drafts of the bill would have included privacy protections applicable to business as well as the government along the European model. Passage of the bill as proposed met stiff resistance from business as well as President Ford. The eventual law applied only to the public sector. Although the Europe-wide Data Protection Directive did not exist until 1995, several individual countries had privacy protections of the type that would later be enshrined in the Directive. Newman, *supra* note 1 at 49 – 50.

[147] Privacy Act of 1974, *supra* note 143.

[148] *Condon v. Reno* (1998), 155 1998 F 3d 453 (rev'd on other grounds); *Reno v. Condon* (2000), 528 2000 US 141.

[149] Condon v. Reno, *supra* note 148.

[150] *Dwyer v. American Exp. Co.* (1995), 652 1995 NE 2d 1351(credit card spending habits); *Shibley v. Time, Inc* (1975), 45 1975 Ohio App 2d 69(magazine subscriber lists).

[151] Newman, *supra* note 1 at 48 – 52.

became politically impossible. The United States remains a holdout with a "sector-specific" privacy regime.[152]

### 8.2.1 Data about children collected online

The Children's Online Privacy Protection Act (COPPA), for example, governs websites that target and collect data from children. Enacted in 1998, this statute requires websites targeting children under 13 to post privacy policies and to obtain parental consent before collecting information from children. Protections for children are easily circumvented, for example by lying about one's age.[153] Several authors associated with Harvard's Berkman Center recently commented that a leading effect of the COPPA has been to turn parents and children into liars – and possibly criminals if the Justice Department's interpretation of the Computer Fraud and Abuse Act is correct.[154] Enforcement of the Act rests with the FTC, which has pursued claims against several companies leading to several fines, the two largest being against the social

[152] Ryan Moshell, "And then there was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection" (2005) 37 Texas Tech L Rev 357; Newman, *supra* note 1.

[153] Theoretically, those under 18 are prohibited from using Google services, including gmail, youtube, and the new Google+. Google previously claimed that users must be able to form a binding contract with Google, which would imply an age of 18 under the laws of all 50 states. However, Google has also at times stated that children as young as 13 can use services such as gmail. "Google Terms of Service – Policies & Principles – (Former version dated April 16, 2007)",, online: <http://www.google.com/intl/en/policies/terms/archive/20070416/>; Google's newest terms of service state that "Our Services are very diverse, so sometimes additional terms or product requirements (including age requirements) may apply. Additional terms will be available with the relevant Services, and those additional terms become part of your agreement with us if you use those Services. "note 68; Use of services by children of all ages is believed to be widespread. Joel Fernandes, "Creating a Google Plus Account Now Requires You to Enter Your Birthday", *Techie Buzz* (27 August 2011), online: <http://techie-buzz.com/social-networking/google-age-restrictions.html>; The FTC offers advice on complying with COPPA. "How to Comply with the Children's Online Privacy Protection Rule | BCP Business Center", (December 2006), online: *Federal Trade Commission Bureau of Consumer Protection* <http://business.ftc.gov/documents/bus45-how-comply-childrens-online-privacy-protection-rule>; For a highly critical look at the effectiveness of U.S. protections for childrens' data, see, Dana Slaughter & Wang Zhenlin, "Information Security of Children's Data: From 'Ego' to 'Social Comparison' - Cultural Transmission and Child Data Protection Policies and Laws in a Digital Age" in *Harboring Data: Information Security, Law, and the Corporation* (Stanford: Stanford University Press, 2009).

[154] danah boyd & Eszter Hargittai, "Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'" (2011) 16:11 First Monday, online: <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075>.

networking site Xanga for $1 million and $400,000 from UMG Recordings.[155] More recently, the FTC has issued a general warning to makers of apps directed at children.[156] Any cloud service marketing to children or with actual knowledge that it is collecting information from children under age 13 will need to be mindful of the requirements of COPPA.

### 8.2.2 Banking information

Because of the third party doctrine of the fourth amendment, there is no general expectation of privacy in banking records.[157] However, the Gramm Leach Bliley Act, which overhauled many banking regulations, contained sections relating to banking information.[158] Banks must give consumers notice of their information sharing policies and also the ability to opt-out of information sharing schemes. The FTC is the primary enforcer of the privacy protection aspects of GLBA. Enforcement actions have included a complaint from the FTC that violations of the GLBA constituted deceptive and unfair trade practices. [159] The FTC defines "financial institutions" broadly, including having tried unsuccessfully to apply the GLBA to attorneys who hold client funds.[160] The GLBA contains rules limiting the sharing of information with any "unaffiliated third party."[161] Any financial institution that does so must notify customers of its

---

[155] Xanga, "Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule", (7 September 2006), online: *Federal Trade Commission* <http://www.ftc.gov/opa/2006/09/xanga.shtm>; UMG, "UMG Recordings, Inc. to Pay $400,000, Bonzi Software, Inc. To Pay $75,000 to Settle COPPA Civil Penalty Charges", (13 September 2006), online: *Federal Trade Commission* <http://www.ftc.gov/opa/2004/02/bonziumg.shtm>. <http://www.ftc.gov/opa/2004/02/bonziumg.shtm>

[156] *Mobile Apps for Kids: Current Privacy Disclosures are Dis**app**ointing* (Washington, DC: Federal Trade Commission, 2012) online, <http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf>.

[157] *United States v. Miller* (1976), 425 1976 US 435.

[158] *Financial Services Modernization Act of 1999*, 1999, 15 USC § 6801 - 6809 [*Gramm Leach Bliley Act*].

[159] "In the Matter of Superior Mortgage Corp., File No. 052 3136",, online: *Federal Trade Commission* <http://www.ftc.gov/os/caselist/0523136/0523136.shtm> The mortgage company had collected information in a secure, encrypted fashion online. However, once the data was collected, company workers emailed it in plain, readable, unencrypted text. "In the Matter of Superior Mortgage Corp., File No. 052 3136 (Consent Order)", (28 September 2005), online: *Federal Trade Commission* <http://www.ftc.gov/os/caselist/0523136/0523136.shtm>(consent order).

[160] *American Bar Ass'n v. FTC* (2005), 430 2005 F 3d 457.

[161] Gramm Leach Bliley Act, *supra* note 158 , section 6802(a).

practices and give customers the right to opt out of such sharing. The question has not been tested, but if a cloud provider was deemed to be an "unaffiliated third party" the financial institution would have to give customers the right to opt out of having their data stored in cloud vendors' systems. Despite the possible difficulties, cloud providers have begun to offer services advertised as GLBA-compliant.[162] The security requirements of the GLBA also require financial institutions to maintain a "comprehensive information security program", which serves to underscore the importance of choosing a reliable cloud provider. Bank records also receive some protection from government searches based on the Right to Financial Privacy Act.[163]

### 8.2.3 Health information

One of the more well known areas in which privacy is protected is health records under the Health Insurance Portability and Accountability Act (HIPAA). This act sets out various protections for health data, when stored by covered entities. The definition of covered entities, however, contains important qualifications. HIPAA "covered entities" include only "(1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards."[164] Thus, a private cloud serving such a "covered entity" might need to be HIPAA compliant. The now-defunct Google Health operated outside HIPAA regulation because it gathered health information from consumers.[165] Microsoft, however, aiming to gain "covered

---

[162] Penny Crossman, "Fieldpoint Private Bank Turns to Cloud Computing for CRM and Beyond - Bank Systems & Technology",, online: *Banktechcom* <http://www.banktech.com/business-intelligence/225702942>; Lamont Wood, "Cloud computing and compliance: Be careful up there", *Computerworld* (30 January 2009), online: <http://www.computerworld.com/s/article/9126934/Cloud_computing_and_compliance_Be_careful_up_there_>.

[163] *Right to Financial Privacy Act.*, 1978, 12 USC 3401 et seq [*RFPA*] (Widely seen as a reaction to Miller).

[164] "HIPAA Privacy Rule and Its Impacts on Research", (2 February 2007), online: *US Dept of Health and Human Services, National Institutes of Health* <http://privacyruleandresearch.nih.gov/pr_06.asp> (Explaining rules contained in 45 CFR 160.103).

[165] Google explained its policy in part with the following:

"Google Google Health and HIPAA

Unlike a doctor or health plan, Google Health is not regulated by the Health Insurance Portability and Accountability Act (HIPAA), a federal law that establishes data confidentiality standards for patient health

entities" (such as Tampa General Hospital, an early customer touted in its advertising) as customers for its Office 365 service promised to be HIPAA compliant. [166] HIPAA-covered entities using cloud providers will have to be mindful to secure terms of service that can guarantee the information will be handled in a compliant manner. For example, a covered entity could not allow a cloud provider to use data entrusted to it for its own purposes.

### 8.3 Other areas

Other bands of privacy protection exist for other areas including; information collected for state drivers licenses,[167] video rental history,[168] education information,[169] credit reporting,[170] and

---

information. This is because Google does not store data on behalf of health care providers. Instead, our primary relationship is with the user. Under HIPAA, patients have a right to obtain a copy of their medical records. If they choose to use Google Health, we'll help them store and manage their medical records online.
Although Google Health is not covered by HIPAA, we are committed to user privacy and have in place strict data security policies and measures, and ensure that users control access to their information. We let users know what information we collect when they use Google Health, how we use it, and how we keep it safe. Users choose who views or adds information to their profile, and they can revoke access at any time.
There is no advertising in Google Health. We do not sell user health information, and we do not share it with other individuals or services unless a user explicitly authorizes us to do so, or in the limited circumstances described in our privacy policy. A user's personal medical records are stored in their secure account and cannot be accessed by others through a search on Google.com. Also, no personal or medical information stored in a user's Google Health profile is used to customize their Google.com search results."
"Google Health and HIPAA", online: *Google Health* <http://www.google.com/intl/en_us/health/hipaa.html>.

[166] Microsoft explained its policies in part with the following:
Due to the requirements of HIPAA, the Health & Life Sciences industry requires privacy, security, and confidentiality of patient data ("protected health information"). With this in mind, Microsoft will be among the first in industry to offer a Business Associate Agreements (BAA) as an operationalized part of its solution to address requirements associated with hosting protected health information. Customers can obtain more information on BAA availability from their designated Microsoft account manager.
One of Office 365's early adopters is Tampa General Hospital, which serves more than 4 million people in Florida. They'll take advantage of Office 365's core productivity solutions – including Microsoft Office, SharePoint, Exchange, and Lync – via the cloud, so that their physicians, nurses and support staff can work wherever they are via whatever PC, browser, or device they're using in a way that works for their business. And, Microsoft manages all of the deployment, maintenance and ongoing support so they can concentrate on their patients.
"Microsoft's Office 365 Cloud Service Goes Live Worldwide - Microsoft in Health - Site Home - MSDN Blogs", (28 June 2011), online: *MSDN* <http://blogs.msdn.com/b/microsoft_in_health/archive/2011/06/28/microsoft-s-office-365-cloud-service-goes-live-worldwide.aspx>.

[167] 18 USC §2721

[168] 18 USC §2710

[169] 20 USC §1232

[170] 15 USC §1681

other niche fields. Most of the specific protections are limited to such a degree as to only be of concern to entities in specific fields. For example, only schools that receive federal funds need concern themselves with the requirements of the Family Education Rights and Privacy Act. These rights generally do not contain a private right of action, meaning citizens must wait for the government to file claim on their behalf. The FTC's broadest authority is under its mandate to police "deceptive" trade practices, although the agency can also enforce some of the other laws. Other agencies, such as the Department of Health or Department of Education also wield authority within specific fields.

### 8.4 FTC Enforcement

The backstop to most U.S. privacy regulation is the possibility of enforcement by the Federal Trade Commission for deceptive trade practices in the form of violations of promises to consumers. These promises can be made in the company's privacy policy, user agreements, marketing material, or other media. Overall enforcement has not always been vigorous. For example, the FTC approved the sale of consumer financial information by the bankrupt retailer Toysmart despite promises to consumers it would not do so. Likewise, the FTC refused to seek fines against Amazon.com for practices that "likely were deceptive."[171]

Some have described FTC enforcement as toothless.[172] However, recent FTC actions securing agreements including concessions and periodic audits of both Google and Facebook for 20 year periods may indicate a growing interest in protecting consumer privacy.[173] The Google

[171] Moshell, *supra* note 152..

[172] *Ibid*.

[173] "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network; Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data", (30 March 2011), online: *Federal Trade Commission* <http://www.ftc.gov/opa/2011/03/google.shtm>; "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises", (29 November 2011), online: <http://ftc.gov/opa/2011/11/privacysettlement.shtm>; Google is also the subject of a seperate antitrust investigation.) Thomas Catan & Amir Efrati, "Feds to Launch Probe of Google", *Wall Street Journal* (24 June 2011), online: <http://online.wsj.com/article/SB10001424052702303339904576403603764717680.html>.

settlement, over the company's "Buzz" social feature – widely seen as a privacy nightmare and commercial disaster – has given the FTC and privacy advocates some leverage. Google has been forced to defend its upcoming privacy policy changes against charges that they violate the 2011 settlement over Buzz.[174] Nevertheless the agency can be slow, perhaps in part due to budgetary constraints.[175] Furthermore, in the United States enforcement of privacy promises is only one of many items on the FTC's plate. Countries with a privacy or data protection commissioner – a group that includes all of Europe, Canada, and many other nations – have an office dedicated strictly to privacy protections. Finally, the FTC has no authority to act unless a company violates its own promises to consumers or one of the limited areas covered by federal protections over which it has jurisdiction.

**8.5 State Protections:**

California led the way in instituting a data breach law, which became effective in 2003. The law requires holders of personal data of California residents to notify the subjects of the data if their information is compromised.[176] Since 2003, when the law took effect, most other states have followed suit.[177] With some variations on the theme, state data breach notification laws require notification either in person, by publication, or through a state's attorney general or other official, whenever personal data is compromised.[178] California's law, although the first,

---

[174] "Google says its new privacy policy complies with FTC settlement", *latimescom* (10 February 2012), online: <http://www.latimes.com/business/technology/la-fi-tn-google-privacy-ftc-20120210,0,5736133.story>.

[175] Christopher Soghoian, "slight paranoia: How long does it take for the FTC to investigate a company?", (February 2012), online: *Slight Paranoia* <http://paranoia.dubfire.net/2012/02/how-long-does-it-take-for-ftc-to.html>.

[176] *California Security Breach Notification Law, SB 1386*, 2003, California Civil Code 1798.29, 1798.82, 1798.84 [*California Security Breach Notification Law, SB 1386*].

[177] "State Security Breach Notification Laws", (6 February 2012), online: *National Conference of State Legislatures* <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>.
(National Council of State Legislatures list of data breach laws by state.)

[178] California Security Breach Notification Law, SB 1386, *supra* note 176."Personal data" is defined in California rather narrowly as follows: "(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(1) Social security number.
(2) Driver's license number or California Identification Card number.

had been overtaken by other states with tougher provisions, such as required notice to state attorneys general. A revision effective as of Jan. 1, 2012 toughened the law.[179] Data breach notification laws do not stipulate any particular measures a company must take to prevent a breach. Also, once a breach has occurred, it is up to consumers (data subjects) to take remedial action.[180] From a consumer's perspective, the utility of such laws could be questioned. However, by publicizing company failings they have at least created market incentives to improve security to avoid public embarrassment or loss of goodwill.[181]

Massachusetts recently enacted a new type of data protection law that not only mandates disclosure of breaches but also standards and practices for covered entities holding personal data of Massachusetts residents.[182] The law is also extra-territorial in that it applies to custodians of data on Massachusetts residents wherever they are located.[183] Several states also have more stringent laws relating to health records than the federal HIPAA. Those that are more stringent and not contrary to HIPAA are not preempted. If one cannot comply with both the state law and HIPAA, the law is "contrary" to HIPAA and preempted.[184] Otherwise, it is not preempted.[185] States also have a number of widely varying protections secured through various statutes. These include laws in California protecting the privacy of online activity, a few

---

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."

[179] See http://www.huntonprivacyblog.com/2011/09/articles/security-breach/california-bulks-up-security-breach-notification-requirements/

[180] For example, potentially costly credit report monitoring.

[181] For a critical look, as well as data breach statistics, see; Andrea M Matwyshyn, "Introduction" in *Harboring Data: Information Security, Law, and the Corporation* (Stanford: Stanford University Press, 2009).

[182] *Massachusetts General Law Chapter 93H*, 2009 [*Massachusetts General Law Chapter 93H*].

[183] Jeffrey D Neuburger & Natalie Newman, *The Bay State Raises the Bar on Personal Data Security: Are You in Compliance?* (Washington, DC: Washington Legal Foundation, 2010).

[184] *45 C.F.R. 160.202*, 2000, Code of Federal Regulations (US) [*45 C.F.R. 160.202*](Definition of "preemption" for relevant purposes).

[185] See, "Preemption by/of state laws (HIPAA)", (2005 2002), online: *University of Miami, Miller School of Medicine Privacy / Data Protection Project* <http://privacy.med.miami.edu/glossary/xd_state_preemption.htm>; See also, Cheryl S Camin, "HIPAA: To Preempt or Not To Preempt? That is the Question (Especially in Litigation)", (2005), online: *ABA Health eSource* <http://www.americanbar.org/newsletter/publications/aba_health_esource_home/Volume2_vol2no1_camin.html>.

state laws protecting information held by Internet service providers, two states with laws requiring that employees be notified if their work email use is subject to surveillance, a few laws mandating privacy policies for commercial websites, and 17 states requiring privacy policies for government websites.[186]

### 8.6 Government access

One fact that some have seen as problematic for cloud computing is that disclosure of information to cloud providers renders it more susceptible to government access. This is compounded by the third party doctrine of fourth amendment law. The third party doctrine is a concept in American constitutional law whereby fourth amendment protection from search and seizure is waived when information is shared with a third party. This holds true even if the information was given in confidence.[187] The third party doctrine has been widely criticized, including recently by Justice Sotomayor. However, a case can be made in its defense.[188] Due to negative public reactions to findings that certain areas do not receive Fourth Amendment protection, statutory protection has been extended to several areas. This has included wiretaps, bank records, and electronic communications under the Electronic Communications Privacy Act.[189]

---

[186] See, "State Laws Related to Internet Privacy", (2012), online: *National Conference of State Legislatures* <http://www.ncsl.org/issues-research/telecom/state-laws-related-to-Internet-privacy.aspx>.

[187] "United States v. Miller, *supra* note 157("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

[188] See, Orin Kerr, "The Case for the Third Party Doctrine" (2009) 107 Mich L Rev 561, online: <http://mlr.stereodevelopment.com/assets/pdfs/107/4/kerr.pdf>.

[189] Wiretaps: *Olmstead v. United States* (1928), 277 1928 US 438 found no Fourth Amendment protection in telephone conversations. Wiretaps are now governed by provisions of the Omnibus Crime Control and Safe Streets Act of 1968, 47 USC § 3711.
(*Olmstead* provided the opportunity for Justice Brandeis memorable dissent expressing concern about the erosive effects of new technology on privacy. For example, "Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." Olmstead v. United States, *supra* note at 473.).
Bank records: United States v. Miller, *supra* note 157. found no Fourth Amendment protection. Bank records are now statutorily protected from government search by the Right to Financial Privacy Act.

Also, when an area of law does not receive the complete protection of the Fourth Amendment, a custom-tailored level of protection can be created by statute. Thus, wiretap warrants are rather difficult to obtain as are the contents of communications under the Electronic Communications Privacy Act. Financial records and electronic communications receive some protection, but rather less than they would if they were covered under the Fourth Amendment.[190]

Several states have rejected the third party doctrine under their state constitutions.[191] Thus, some information stored "in confidence" in the cloud may receive greater protections than under federal law. The Fourth Amendment applies only to government actors. However, some of the Fourth Amendment-like protections under ECPA also apply to private actors or in civil suits. In such a case, information protected from discovery by a subpoena to a third party will likely be discoverable by a discovery production request.[192]

**8.7 Possible reforms:**

Companies engaged in cloud computing have testified about what they see as the needed reforms to foster economic growth in the cloud.[193] The biggest request is for reform of the Electronic Communications Privacy Act (ECPA), a 1986 law governing privacy of electronically stored information that many say has not withstood the test of time. ECPA provides some

---

Email. Fourth amendment protections do not apply to email. However, under the Electronic Communications Privacy Act sections of the Stored Communications Act ECPA, *supra* note 113., Congress has created an elaborate scheme of varying degrees of protection based on the age of communications, their status (opened or not), and type.

[190] See, Kerr, *supra* note 188.

[191] *Ibid*.

[192] *Flagg v. City of Detroit*, 252 FRD 346.(Text messages protected by ECPA 28 USC 2701. Civil suit plaintiff ordered to convert third party subpoena to phone company into Rule 34 discovery request to defendant.)
See also, Timothy G Ackermann, *Consent and Discovery Under the Stored Communications Act* (2009) online, <http://www.pattersonsheridan.com/images/uploads/SCA_Control_article_PUBLISHED-crop.pdf>.

[193] "Digital Due Process: Modernizing Surveillance Laws for the Internet Age", (2010), online: *Digital Due Process* <http://digitaldueprocess.org/index.cfm?objectid=FE5C92F0-2552-11DF-B455000C296BA163>.

limited protection from government searches of electronically stored material. It was widely seen as intended to promote growth of then-new industries. This was necessary, because under the third party doctrine, law enforcement agents do not need a warrant to compel disclosure of information entrusted to another.[194] ECPA is seen as intended to promote confidence in electronic communications.[195] In a historical antecedent, phone companies in 1928 argued for the extension of Fourth Amendment protection to phone calls to inspire consumer confidence.[196]

Even many of those who laud the intentions behind ECPA often argue that it needs updating to reflect the technology of today.[197] Although there is widespread agreement from industry that the law needs amendment, requests range from increasing substantive protections to merely updating language to keep pace with technology. Even more solid protection would be afforded if the third party doctrine were abandoned. Although this is not likely, Supreme Court Justice Sonya Sotomayor recently noted the difficulties presented by the doctrine in an age when so much information is entrusted to others electronically;

> *[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers*.[198]

---

[194] See Kerr, *supra* note 188.

[195] According to testimony of Microsoft Associate General Counsel Mike Hintze before the Judiciary Committee of the U.S. Congress, ECPA "[struck] a balance between the legitimate needs of law enforcement and the public's reasonable expectations of privacy." *ECPA Reform and the Revolution in Cloud Computing*, Mike Hintze, 23 September 2010 [*ECPA Reform and the Revolution in Cloud Computing*] online, <http://judiciary.house.gov/hearings/hear_100923.html>.
Mr. Hintze stated later that today; "Users of cloud computing services must have confidence that their data will be keep secure and private not just vis-à-vis the government but also with respect to service providers and other third parties."

[196] See, Olmstead v. United States, *supra* note 189 , note 12.

[197] Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It* (Washington, DC: George Washington University Law School, 2004)..

[198] *US v. Jones* (2012), 132 2012 S Ct 945.

Additionally, ECPA has been interpreted differently by different courts. The 9th Circuit – whose territory includes some of the biggest cloud providers in the world – has interpreted ECPA to provide considerably more protection than other circuits.[199]

Senators John Kerry and John McCain have also introduced a bill that would mandate a federal data protection plan for the United States.[200] However, critics say the so-called "Consumer Privacy Bill of Rights" would pre-empt many stronger state protections and do little to protect consumers.[201] Notably, there would be no private right of action for privacy breaches. Enforcement would be in the hands of the Commerce Department, which is generally seen as business-friendly. President Obama recently announced his plans for a Consumer Privacy Bill of Rights.[202] The president's plan would seemingly involve a combination of industry self-regulation and baseline protections imposed by Congress.[203] Kerry has endorsed Obama's efforts.[204]

---

[199] *Theofel v. Farey-Jones* 359 F.3d 1066 (2004).
See Orin S. Kerr, *A User's Guide*, above, for criticism.

[200] "John Kerry - United States Senator for Massachusetts : At Work for You in Congress - List of All Issues - Commercial Privacy Bill of Rights", (12 April 2011), online: *Kerrysenategov* <http://kerry.senate.gov/work/issues/issue/?id=74638d00-002c-4f5e-9709-1cb51c6759e6&CFID=79733731&CFTOKEN=26547080>.

[201] See, "How Would the Kerry-McCain 'Commercial Privacy Bill of Rights' Affect State Security and Privacy Laws?", (20 May 2011), online: *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2011/05/how-would-kerry-mccain-commercial-privacy-bill>.
For a more favourable account, see; "Department of Commerce Official Asks Congress to Enact 'Privacy Bill of Rights'", (16 March 2011), online: *Privacy and Information Security Law Blog* <http://www.huntonprivacyblog.com/2011/03/articles/department-of-commerce-official-asks-congress-to-enact-privacy-bill-of-rights/>.

[202] Barrack Obama, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (The White House, 2012).

[203] *Ibid*.

[204] "Kerry Statement on Obama Privacy Bill of Rights", (23 February 2012), online: *Kerry.senat.egov* <http://kerry.senate.gov/press/release/?id=36D3DCC0-9FD8-4A0A-BA5B-ED411C97E108>.

### 8.8 Industry efforts

Cloud computing providers have been pressing for various reforms to give consumers greater confidence in the cloud.[205] Many of the biggest providers – together with other groups such as the ACLU and Electronic Frontier Foundation – have joined the Digital Due Process Coalition, a group primarily interested in ECPA reform.[206] Microsoft, also a member of the Digital Due Process Coalition, has also released its own goals for legal reform.[207] On Sept. 23, 2011, representatives of several companies testified before the House Committee on the Judiciary at a hearing captioned "ECPA Reform and the Revolution in Cloud Computing."[208] Generally, tech providers agree that ECPA needs to be updated to reflect modern technology. However, providers are divded on whether the statute needs to be strengthened so as to provide substantively more protections.

Companies would also like to see strengthening of anti-hacking provisions, especially the Computer Fraud and Abuse Act. This could include changes to allow aggregation of damages to more easily make offenses felonies. It could also include granting providers a private right of action. Currently hosting companies do not have a private right of action to go after hackers. While their customers do, hosting companies generally do not.[209] Companies have also asked

[205] note 193.

[206] www.digitaldueprocess.org

[207] *Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing* (Microsoft, 2010); *Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing* (Microsoft, 2010).

[208] ECPA Reform and the Revolution in Cloud Computing, *supra* note 195. The witnesses included representatives of Google, Microsoft, Salesforce.com, Rackspace Hosting, and Amazon.com. Most of the industry witnesses identified their companies as members of the Digital Due Process Coalition. Two academics and one practicing lawyer gave testimony generally in accord with the industry representatives. Two law enforcement officials who testified questioned the wisdom of increased privacy protections in the cloud.

[209] According to the testimony of Microsoft's representative under questioning, it is the providers who "have resources and the incentives to really go after the hackers." (Testimony of Mike Hintze, Microsoft, at p. 76).

Congress to clarify the rules and process for bulk data requests, [210] for real time communications interceptions,[211] and jurisdictional rules. [212]

### 8.9 The challenges of the USA Patriot Act

American cloud providers must face the difficulties of complying with the laws of other countries, especially European countries, when serving foreign customers. This can be challenging on its own for American companies. While many of the world's top cloud providers are American, their marketing has been made more difficult by a general distrust in the American approach toward data and privacy protections, and more specific fear of the USA Patriot Act.[213] Citizens, government, and users in many countries have expressed their concerns about using any service that is based in, or routes through the U.S. The level of criticism is likely exaggerated, especially given that every country has provisions similar to the Patriot Act allowing interception of communications.[214] Legislation even more intrusive than the Patriot Act was recently defeated in Canada in the form of the Lawful Access bill.[215] In a surprising turn of events, the majority Conservative government was forced to withdraw the bill in February, 2012. A similar bill in the UK introduced in 2012 is inspiring similar levels of public concern.[216] Additionally, even the European Data Protection Directive does not apply to measures intended to enforce investigations or national security. According to its terms, the directive exempts "processing operations concerning public security, defence, State security

---

[210] Bulk data requests include instances when the government asks a provider for a large amount of information from numerous users, such as "everyone who visited website x between the following dates" or "your last one million search requests."

[211] For example, a series of backward-looking requests to produce emails or other electronic communications could serve as the functional equivalent of a wiretap order, but with a much lower showing from the government.

[212] note 207; note 207; note 193.

[213] Zack Whittaker, "Microsoft admits Patriot Act can access EU-based cloud data", *ZDNet* (28 June 2011), online: <http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225>.

[214] For example, The Rt Hon Sir Paul Kennedy, *2010 Annual Report of the Interception of Communications Commissioner* (Parliament of the United Kingdom, 2011).

[215] *Protecting Children from Predators Act*, Vic Toews, February 2012 [*C-30*].

[216] "GCHQ: Big Brother plans to let state spy on websites, emails and texts to cost YOU £2bn", *Mail Online*, online: <http://www.dailymail.co.uk/news/article-2124251/GCHQ-Big-Brother-plans-let-state-spy-websites-emails-texts-cost-YOU-2bn.html>.

(including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law."[217] It seems that concerns about the Patriot Act may be vastly overblown and/or mixed with anti-American or anti-market leader sentiments. At least a certain amount of resistance to using American cloud providers in other countries must be attributed to the Patriot Act.[218] Justly or not, the Patriot Act is a marketing headache for American cloud providers.[219] American providers had been building data centers in European countries to claim to be within the European Economic Area for purposes of complying with the DPD. However, it has become increasingly clear that as companies based in the United States they are not out of the range of the Patriot Act.[220]

---

[217] "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard, (a) national security (b) defence, (c) public security;" (the list goes on to include even more mundane things like investigating regular crimes and members of regulated professions. 95/46/EC, *supra* note 85 Article 3(2).

[218] Jenni Kavur, "Don't use the Patriot Act as an excuse", *ComputerWorld Canada* (5 July 2010), online: <http://www.itworldcanada.com/news/dont-use-the-patriot-act-as-an-excuse/141033>; David TS Fraser, "Canadian Privacy Law Blog: Patriot Act reality check and Canadian authorities' similar powers", (28 April 2010), online: *Canadian Privacy Law Blog* <http://blog.privacylawyer.ca/2010/04/patriot-act-reality-check-and-canadian.html>; Kris Klein, *Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act: Transborder Data Flows and their Regulation* (Law Office of Kris Klein for Salesforce.com, 2010).

[219] French provider Filnet proposes "un cloud made in France":
Filnet, "Microsoft 365 et Patriot Act: Filnet appelle les entreprises à choisir un Cloud Made In France | Filnet", (Juillet 2011), online: *Filnetfr* <http://www.filnet.fr/content/microsoft-365-et-patriot-act-filnet-appelle-les-entreprises-choisir-un-cloud-made-france>.
For example, Forrester Research marks the United States as requiring "caution" due to possible government surveillance: "Forrester's Global Data Protection and Privacy Heatmap", (2011), online: *Forrester Tools* <http://heatmap.forrestertools.com/>.

[220] Chris Whittaker's Patriot Act series (Whittaker, *supra* note 213.) in ZDNet pursued this relentlessly, particularly in light of Microsoft's summer 2011 launch of Office 365.
See also, "Essers, *supra* note 65.

### 8.10 International Customers – E. Discovery

A less sensational, but also real danger of U.S. entanglement for international customers exists because of U.S. discovery law and procedure. Most civil law countries have much more limited discovery procedures managed by courts. Because of blocking statutes and data protection laws that are generally more protective than U.S. law, some potential customers may be unwilling to put their data in their "possession, custody or control"[221] Non-parties may also be compelled to disclose data.

[221] FRCP 34 "A party may serve on any other party a request within the scope of Rule 26(b):
(1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control: (A) any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or…"

## 9. EUROPEAN LEGAL ENVIRONMENT

### 9.1 Privacy regulation

Europe boldly proclaims that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[222] Legislation in every European country restricts the "processing" of information about identifiable individuals[223]. In the United States, on the other hand, even the exchange and mining of data about the prescribing habits of doctors for a commercial purpose is "a form of expression protected by the Free Speech Clause of the First Amendment" and can only be regulated under the strictest of circumstances.[224] Europe's approach to data protection could be caricatured as overly brittle and binary, overburdening business, stifling innovation, and too full of inflexible rules that leave no room for discretion or risk assessment. The American approach, on the other hand, can seem inadequate in its protections of consumers and the public. While Europe protects any data that can be associated to any "identified or identifiable natural person"[225] the U.S. norm is unfettered free speech and free trade in data about people. Only in a few areas seen as especially troublesome – health, children, financial data- are general restrictions in place in the United States.

Generally, Europe privileges protection of privacy to a much greater extent than the United States. To those who support it, data protection and privacy can transcend commercial

---

[222] ECHR 8.1, *supra* note 138.

[223] 95/46/EC, *supra* note 85 Processing is defined broadly: ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Personal data is also defined broadly: "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" The two broad definitions mean that almost anything one can do with information about an identifiable individual is potentially subject to regulation. A number of exceptions (such as for art or journalism or purely non-commercial "household" purposes) exist that take information out of the regulatory scheme. .

[224] *Sorrell v. IMS Health Inc.* (2011), 131 2011 S Ct 2653 (available on http://scholar.Google.ca/scholar_case?case=8380938403992670&hl=en&as_sdt=2&as_vis=1&oi=scholarr).

[225] Some nations extend the protections to legal persons, such as corporations.

interests and speak to issues of human dignity.[226] The importance of data privacy can be seen in the European decision to include privacy among the enumerated human rights in the European Convention on Human Rights.[227] A strand of European thought is illustrated by the statement of the head of the French data protection agency CNIL that "the Europe of trade must not take precedence over the Europe of rights."[228] In the United States, politicians are increasingly referencing the unsettling nature of corporate data mining practices.[229]

### 9.2 A European single market?

The stated aim of the Data Protection Directive passed in 1995 was to permit flows of data within Europe – to create a single market.[230]

> "Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."[231]

Proponents of protective regimes have argued that increasing trust through legislation is an effective way to foster growth in the use of the Internet and e-commerce. To some, the Internet and other "Information Society" services would not have taken off if users hadn't felt

---

[226] Turow, *supra* note 69.

[227] ECHR 8.1, *supra* note 138; See also, James Q Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale L J 1151, online: <http://www.yalelawjournal.org/the-yale-law-journal/content-pages/the-two-western-cultures-of-privacy:-dignity-versus-liberty/>.

[228] Newman, *supra* note 1 at 89.

[229] See, for example, Turow, *supra* note 69; Barrack Obama, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (The White House, 2012); "John Kerry - United States Senator for Massachusetts : At Work for You in Congress - List of All Issues - Commercial Privacy Bill of Rights", (12 April 2011), online: *Kerry.senate.gov* <http://kerry.senate.gov/work/issues/issue/?id=74638d00-002c-4f5e-9709-1cb51c6759e6&CFID=79733731&CFTOKEN=26547080>.

[230] 95/46/EC, *supra* note 85 , paragraph 3; See also Newman, *supra* note 1.

[231] 95/46/EC, *supra* note 85 at 46.

secure in using them.[232] The Data Protection Directive has still not succeeded in creating a single market in Europe and a global single market is even further away. Instead, the world has evolved a mix of laws that create barriers between countries.

### 9.3 The Data Protection Directive

The most striking differences between the U.S. and EU approaches to matters bearing on cloud computing can be seen in the Data Protection Directive, 1995/46/EC. As a directive, the law is applied slightly differently in each EU state, and each state was required to implement the Directive by the end of 1998. Significant variations exist between member states, although all follow the minimum protections outlined in the Directive. For example, some EU nations have met the standards of the Directive with a single data protection law for the public and private sectors, while others have enacted two or more laws for the public and private sectors. Enforcement and penalties also vary by country.[233] The Data Protection Directive principles have also been embraced by the EU plus Norway, Iceland, and Lichtenstein, which are not EU members. The expanded area is called the European Economic Area (EEA). Various provisions of the Data Protection Directive, most importantly the restrictions on transferring data outside the EEA thus include this group of 30, rather than the EU 27.

Data Protection Directive of 24 October, 1995 represented a Europe-wide embrace of a comprehensive data protection regime.[234] The Directive applies to any "processing" of data taking place wholly or partly by electronic means as well as non-automated data that is part of

[232] For example, in explaining the rationale for the proposed new Data Protection Regulation, the European Commission explains; "Building trust in the online environment is key to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services. This risks slowing down the development of innovative uses of new technologies. Personal data protection therefore plays a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy European Commission, *supra* note 91.

[233] The following provides a country-by-country overview, focusing on the implications for litigation: Stefan Hanloser & Catrien Noorda, eds, *E-Discovery and Data Privacy: A Practical Guide* (Alpen aan den Rijn, NL: Wolters Kluwer, 2010).

[234] Contrast this to the U.S. sectoral approach, regulating data held by the government, about children, about certain financial transactions, health, etc., in separate statutes.

a "filing system." "Processing" is broadly applied to include "virtually any activity in respect of personal data…", which is any data about an identifiable individual. [235] According to Article 6 of the Directive, personal data must be;

- Processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Additional heightened restrictions apply to sensitive data, such as data about health, religion, membership in organizations, and political beliefs.

Almost anything one could do with personal data requires a justifying reason, without which it would be illegal. Justifications include;

- The data subject has unambiguously given his consent,
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controlled is subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

[235] Catrien Noorda & Stefan Hanloser, "EU Data Privacy Regulations" in *E-Discovery and Data Privacy: A Practical Guide* (Frederick, MD: Wolters Kluwer, 2011) at 16.

- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed [unless overridden by other interests of the data subject.] [236]

The terms "controller", "processor", and "subject" are important in understanding the Data Protection Directive. A subject is the person the data describes. The controller is a legal or natural person who controls the processing of the data. A processor is a legal or natural person who performs some activity on the data for the benefit of the controller.[237] Thus, a cloud productivity suite where the user controlled all the information could likely qualify as a "processor". (The end user would be the "controller.") However, an application such as Facebook that takes user information and uses it for other purposes (such as marketing) would be controlling that data, and would thus be a data "controller". The most detailed requirements of the Directive deal with controllers, but standards for processors are laid out as well. An argument can be made that IaaS providers (i.e. Amazon EC2) should not even be considered processors, but merely providers of equipment or facilities.[238] Laws implementing the Directive impact anything a "controller" of data might do with the data, including for its own use, or for transferring to other entities or out of the European Economic Area. For example, customer lists and employee data would be protected by the Directive. The task of compliance with laws derived from the Directive has become a major issue for companies that do business in Europe.[239]

---

[236] 95/46/EC, *supra* note 85 Article 7.

[237] See Article 29 Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"* (Brussels: Article 29 Working Party, 2010) online, <http://www.cbpweb.nl/downloads_med/med20100219_C.03%20DC-DP_Opinion_ADOPTED.pdf>.

[238] W Kuan Hon, Christopher Millard & Ian Walden, *Who is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2* (London: Queen Mary University of London, School of Law, 2011).

[239] Data protection considerations keep numerous data protection officers employed and are the subject of numerous treatises. For example, Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2007).

### 9.3.1 Data Protection Authorities

Each member state has at least one data protection authority (DPA).[240] These authorities issue strongly persuasive, but nonbinding opinions regarding specific practices.[241] The attitude of the local DPA can influence the climate for cloud computing in a jurisdiction. For example, Germany generally, and Schleswig-Holstein specifically are viewed as tough, along with Spain. The nonbinding opinions of the "Article 29 Working Party", composed of representatives of every data protection authority in Europe, are also highly persuasive. Firms often opt to comply with the opinions of the Working Party and avoid litigation in the national courts or regulatory penalties, even though the opinions have no direct regulatory application.[242] A notable recent exception to this has been Google's decision to implement a new privacy policy in March, 2012 despite a statement from the French DPA, CNIL, that the new policy would violate EU law.[243] Google implemented the new policy anyway; it legality is now likely to be tested in court sometime soon.

## 9.4 EU strength in unity

The universal recognition of judgments within the EU is important for cloud computing decision-making. Cloud providers are of course free to ignore markets where the cost of compliance outweighs the potential benefits. If not for European unity, a cloud provider might simply ignore a troublesome jurisdiction. However, no provider is likely to ignore all of

---

[240] Notably, Germany has a federal agency as well as one for each Lander (federal state).

[241] The German DPA of Schleswig-Holstein is notable for its tough stance.
For example, "Cloud Computing in the EU: Getting a grip on the data protection/data security issues", (13 September 2010), online: *Project Counsel* <http://www.projectcounsel.com/?p=646>. (English language account of recent opinion that absent other factors, the use of a cloud outside the EU will be per se illegal if not strictly "necessary." Contains links to German language original and press release.)

[242] Newman, *supra* note 1 at 120.

[243] CNIL had been designated as lead agency in addressing concerns about Google's new privacy policy; Isabelle Falque-Pierrotin, *CNIL Letter to Google* (CNIL, 2012); CNIL public statement CNIL, *Google's new privacy policy raises deep concerns about data protection and the respect of the European law* (Paris: CNIL, 2012); Google France SARL, *Google France Letter to CNIL, April 5, 2012* (Google France SARL, 2012).

Europe.[244] Additionally, EU countries are tolerant of wide claims to jurisdiction in most matters, including civil and criminal matters. [245] It should be borne in mind that the effect of a judgment from a country in which a provider does not have a physical presence must be balanced against the likelihood that it will be enforced. In some matters related to free speech, enforcement in the United States might be problematic, however international recognition of judgments is the rule rather than the exception.[246] In more mundane commercial matters or matters of cooperation with criminal investigators enforcement in the home jurisdiction (i.e., the U.S.) of a cloud provider would be more likely.

---

[244] Jack Goldsmith & Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford: Oxford University Press, 2006), chapter 10.(The authors compare Europe's status in privacy regulation worldwide to that of California in regulating automobile emissions in the U.S. Because California has enacted stricter environmental standards than the federal government and because California is too big to ignore, the state effectively sets environmental standards for the entire United States.)

[245] See, *Association Union des Etudiants Juifs de France v. Yahoo! Inc.* (2000), 6 2000 ILR Nov. 20, 2000 434.
In data protection matters, the Data Protection Directive will apply to data controllers outside the EU any time data is collected by "means" or "equipment" within the EU. Those terms are taken to include cookies used in a web browser. An expected revision of the Data Protection Directive will likely include a provision clarifying that it applies to non-EU companies that target EU residents. ("EUROPA - Press Releases - Viviane Reding Vice-President of the European Commission, EU Justice Commissioner The reform of the EU Data Protection Directive: the impact on businesses European Business Summit Brussels, 18 May 2011", (18 May 2011), online: *Europa* <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/349&format=HTML&aged=1&language=EN&guiLanguage=en>.See also, two more recent cases from Belgium: "Yahoo vs. Belgium" *PROCUREUR-GENERAAL BIJ HET HOF VAN BEROEP TE GENT, eiser, tegen YAHOO! Inc.*, 2010 Nr P101347N (available on http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20110118-1)(in Flemish). The case involving a fine for Yahoo for not adequately cooperating with criminal investigators turned on whether Yahoo! was a communications provider. The mid-level appellate court held that Yahoo! was not, as the national telecom provider was the only Belgium communications provider. (Communications providers are obligated to provide certain information to criminal investigators.) Notably, Yahoo!'s presence in Belgium for purposes of jurisdiction was never questioned despite the fact that Yahoo! has no physical presence in Belgium.
See also, "Google vs. Belgium": Google was ordered to stop linking certain Belgian newspapers through its search service. Notably, Belgium took jurisdiction, again despite Google's protests that U.S. law should apply. Notably, the Belgian publisher's group pointedly did not avail itself of the universally recognized "robots.txt" protocol signaling a desire not to be included in search engines. To date, Google has never ignored a robots.txt request.

[246] For example, in the case of Yahoo!'s Nazi memorabilia fines imposed by France, the District Court noted that, it is extremely unlikely that any penalty, if assessed, could ever be enforced against Yahoo! in the United States."*Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme* (2001), 169 2001 FSupp2d 1181; The case was later overturned on ripeness grounds. Consequently, the 9th Circuit did not address the enforceability of the French fines in the United States; *Yahoo! Inc. v. La Ligue Contre Le Racisme* (2006), 433 2006 F 3d 1199.

### 9.5 Advertising-supported services

The directive's requirements can have a burdensome effect on the advertising-based business model. Services such as Facebook and Google monetize their "free" services at the cost of personal data used to sell targeted advertising. Generally, this will require justification by consent. However, the requirements of Article 6 will still apply, including that the data be used only for the purposes for which it was gathered (for which permission was originally given) and that it be "kept no longer than is necessary for the purposes for which the data were collected…" If personal data can be effectively anonymised, it will no longer be covered under the Directive.[247] Data is "personal data" if it relates to an "identified or identifiable natural person".[248] This means that information need not be attached to names to be considered personal data. In a common example, IP addresses are generally considered to be personal data. Data cannot be assumed to no longer be personal data merely because names have been removed.[249]

Both Google and Facebook have come under scrutiny. Google was forced to curtail the amount of time it retained search data[250] and also to add a "privacy" link to its famously sparse homepage. At the very least, companies seeking to monetize personal data must be careful to seek permission for any purpose for which they intend to use personal data. Privacy protections in the European Union probably also have a negative effect on the value of targeted ads. For example, one 2010 research paper reported that such ads were 65 percent less valuable in Europe than in the United States because advertisers do not have the benefit of the

[247] Hon, Millard & Walden, *supra* note 238.

[248] 95/46/EC, *supra* note 85 Article 2(a)(2).

[249] Opinion 1/2008 on data protection issues related to search engines Article 29 Working Party, *supra* note 139 , note 2. The Working Party referred specifically to the 2006 "AOL case" when a journalist successfully determined put names to many allegedly anonymous search records released by AOL.
See, Viktor Mayer-Schönberger, *Delete: the virtue of forgetting in the digital age* (Princeton University Press, 2009), chapter 1.

[250] Article 29 Working Party, *supra* note 139; "How long should Google remember searches?", (12 June 2007), online: *Google Official Blog* <http://googleblog.blogspot.ca/2007/06/how-long-should-google-remember.html>; "Google limits the search data retention period", (28 March 2007), online: *EDRI Digital Civil Rights in Europe* <http://www.edri.org/edrigram/number5.6/google-data-retention>.

rich pools of personal data necessary to target ads, as is common in the United States.[251] Since such ads represent all or nearly all of the income stream of services like Facebook or Google, it is easy to see how this could negatively impact bottom lines.

Although the basic law across Europe is similar, cloud providers may find variation from jurisdiction to jurisdiction based on the attitude of the local DPA or variations in national law. While many companies take advantage of the so-called "Safe Harbor Program" to transfer data to the U.S., the treatment of proposed transfers under the program can be treated differently in each European country.[252] Despite the harmonizing intentions of the Data Protection Directive, Europe still has not achieved a true single market in terms of data protection.[253]

Importantly for social networking sites, such as Facebook, many or most users operate under the so-called "household exemption." To the extent that they operate within "a purely personal sphere", data protection laws do not apply.[254] Thus, the activities of the average Facebook users are not governed by the Data Directive. [255] However, the Working Party noted an increasing trend of using social networking pages as a marketing device, in which case the household exemption would not apply. For example, the Facebook page of a business would not qualify for the household exemption. In some cases, the distinction is not so clear. For

---

[251] Avi Goldfarb & Catherine Tucker, "Privacy Regulation and Online Advertising" (2010) SSRN eLibrary, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259>.

[252] Under the Safe Harbor Agreement, U.S. companies agree to abide by certain standards. Compliance is monitored by the Federal Trade Commission. "Safe Harbor - List", (2012), online: *Export.gov* <https://safeharbor.export.gov/list.aspx>.
The program is meant to provide a basis for what would otherwise be impermissible transfers to the U.S. Google notes "acute" differences in the administration of the program between different European countries. Google, *Google Contribution to the Public Consultation on Cloud Computing* (Brussels, 2011). )

[253] This is cited as a reason for replacing the Directive with a regulation. See; European Commission, *supra* note 91.

[254] See Opinion 5/2009 "On Online Social Networking"
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

[255] In many aspects of cloud computing generally, and social networking specifically, parties can simultaneously be controllers for different aspects of the data. The user who posts data might be a "controller" to the extent that he or she is publishing it to the world. The networking service might also be a "controller" to the extent that it was using the data for other purposes, such as marketing. The household exemption would not be available to a company using the data for marketing.

example, a lawyer in solo practice might have a Facebook page mixing social interactions with marketing.[256] In an important early case, the household exemption was held not to apply to Mrs. Bodil Lindqvist, the "Swedish Church Lady" who was fined for posting gossip about fellow church members on her homemade website as the.[257] Entities may be both "controllers" and "processors" of the same data for different purposes. [258] For example, a customer who places information on a cloud service will be a "controller" of that information inasmuch as he or she controls the information. The cloud service would be a processor. However, if the service makes its own use of the data, for example for targeted advertising, the service will also be a "controller" of the data. Thus, the same person or entity could be controller and processor of the same data for different purposes, and the same data could be have multiple controllers for different purposes.[259] Even if the "household exemption" applies to the first use of the data in the cloud, it will not apply to later commercial uses.

### 9.6 Cross border transfers

Enterprise scale cloud computing faces a different set of challenges. Perhaps the most notable of these is the prohibition on transferring data to countries not deemed to provide adequate protection of personal data. The Working Party periodically reports on the state of data protection law in various countries, pronouncing them either adequate or not. Besides the 30 members of the EEA, a relatively short list of countries, including Canada, Israel, and the Dubai International Financial Center qualify. Restrictions on transfers out of the EU can cause major

---

[256] Article 29 Working Party, *Opinion 5/2009 on Online Social Networking* (Brussels: Article 29 Working Party, 2009).

[257] Edward C Harris, "Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show that Europe Does Not Have the Answers" (2007) 22 Am U Int'l L Rev 745, online: <http://works.bepress.com/edward_harris/2/>.
Note that, as trivial as the offense sounds, the website Mrs. Lindqvist made for the church was not really "household" in that it furthered the goals of an organization – the church. Also, she posted at least two types of sensitive information entitled to heightened protection – religious affiliation and health information. (She mentioned that a parishioner was on half-leave due to an injured foot.)

[258] See, Article 29 Working Party, *supra* note 256.

[259] Article 29 Working Party, *supra* note 237.

problems in a few types of cases. In some cases, restrictions on transfers can pose problems for business, such as limitations on transferring data on customers or employees. In others, they could also result in conflicts between European regulations and those of other countries, often the United States.

### 9.6.1 Common law discovery requests

In American discovery requests, it is not unusual for American discovery and EU data protection laws to clash. It is sometimes impossible not to either be in contempt of an American court or in violation of a European privacy law. [260] A wide range of literature exists regarding this subject.[261] Because much information Americans would consider purely work-related is available on corporate networks, conflicts can arise. Generally, any information about identifiable individuals is protected, even if produced on company time.[262]

### 9.6.2 Blocking statutes

Difficulties in pretrial discovery for American trials are also exacerbated by various "blocking statutes." These statutes either prohibit or severely limit the conditions under which evidence can be gathered in various countries. Blocking statutes generally have their roots either in efforts to protect sovereignty or simply because American-style discovery is unknown to the Continental system. Most countries have procedures in place, such as letters rogatory or the Hague Convention on the Gathering of Evidence Abroad in Civil and Commercial Matters, that can be cumbersome or so time consuming as to preclude use at trial. Companies may become accustomed to the practical ability to move data across national boundaries, although in some instances to do so for litigation might in fact violate the laws of other nations.

---

[260] Article 29 Working Party, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation* (Brussels: Article 29 Working Party, 2009).
[261] Frank P Sedlarcik & Nancy L Hoffman, *Litigating at Home and Fact Finding Abroad* (American Intellectual Property Law Association); Orla Lynsky, Neil Robinson & Michael Greenberg, *e-Discovery and legal frameworks covering Privacy and Data Protection in European countries* (RAND Europe, 2010).
[262] Cavajal, *supra* note 87.

### 9.7 Problems with the U.S.A. Patriot Act

The U.S.A. Patriot Act generally allows U.S. intelligence officials to serve warrants to secure information thought to be related to terrorism. Potential cloud customers have been turned away by fears of American snooping in their data.[263] Such fears generally downplay the fact that almost every nation has some legal mechanism for government access to information in the name of national security.[264] Nevertheless, Patriot Act worries seem to be a headache for U.S. cloud providers.[265] This has led some, such as the Dutch and some German DPAs to question the legality of using American providers.[266] At least one French provider specifically references the Patriot Act to "appelle les enterprises à choisir un cloud made in France."[267] The provider, Filnet, differentiates itself based on its exclusively French establishment. Questions regarding the applicability of the Patriot Act have come to the attention of European Parliamentarians concerned about the issue and will likely continue to be important for the foreseeable future.[268]

### 9.8 Carrier Immunity

In the United States companies benefit from "Section 230" immunity for user-generated content.[269] Carrier immunity in Europe can be more limited than in the United States. Europe

---

[263] Canadian examples include problems with adopting by public bodies such as colleges or healthcare systems. Whittaker, *supra* note 67.

[264] Loek Essers, "Dutch government set to block US cloud IT providers", *CIO* (20 September 2011), online: <http://www.cio.co.uk/news/3304573/dutch-government-set-to-block-us-cloud-it-providers/>.

[265] Whittaker, *supra* note 213.

See the links to the other stories in the series about the PATRIOT Act's extraterritorial effect.

[266] Jonathan P Armstron & Eberhard H Rohm, *Data Protection Regulator for Germany's Schleswig-Holstein Calls for European Review of FTC's Safe-Harbor Program* (2010); Essers, *supra* note 264.

[267] Filnet, *supra* note 219.

[268] See, Sophia in 't Veld, "Written question - Access to EU data by US authorities - E-006901/2011", (13 July 2011), online: *Europarl* <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-006901+0+DOC+XML+V0//EN> (MEP Sophia in 't Veld sought advice as to the ability of U.S. authorities to access information stored in the cloud).

[269] *47 U.S.C. 230*, 1996 [*Communications Decency Act*], section 230.

recognizes a "mere conduit" defense found in the EU Electronic Commerce Directive of 2000. The relevant section states that information service providers will not be liable for information transmitted provided they meet a number of conditions.[270] On its face, the "mere conduit" exception sounds rather like the American provider immunity of the Communications Decency Act.[271] However, the European directive does not apply to matters governed by the data protection directive or the Electronic Privacy and Communications Directive.[272] Thus, cloud providers in Europe face the prospect of being held liable for content posted by their users. This was illustrated in 2010 when several executives of Google Italy received suspended sentences because Google's subsidiary Youtube had unknowingly hosted a video showing a handicapped boy being taunted. The company removed the video as soon as it became aware of it.[273] The prison sentences were possible because the Italian implementation of the Data Protection Directive allows for criminal penalties. This also illustrates an inconsistency in cloud computing law across Europe. For example, UK law implementing the same directive would have provided for only a monetary fine.[274] Google called the ruling a serious threat to the Web;

> European Union law was drafted specifically to give hosting providers a safe harbor from liability so long as they remove illegal content once they are notified of its existence. The belief, rightly in our opinion, was that a notice and take down regime of this kind would help creativity flourish and support free speech while protecting personal privacy. If that principle is swept aside and sites like Blogger, YouTube and indeed every social network and any community bulletin

---

[270] *2000/31/EC*, 2000 [*Directive on Electronic Commerce*].

("1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.").

[271] Communications Decency Act, *supra* note 269("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

[272] Directive on Electronic Commerce, *supra* note 270.

[273] Rachel Danadio, "Larger threet is seen in Google case", *New York Times* (24 February 2010), online: <http://www.nytimes.com/2010/02/25/technology/companies/25google.html>.

[274] "Google convictions reveal two flaws in EU law, not just Italian law", *Pinsent Mansons Out-Law* (3 March 2010), online: <http://www.out-law.com/page-10805>.

> board, are held responsible for vetting every single piece of content that is uploaded to them — every piece of text, every photo, every file, every video — then the Web as we know it will cease to exist, and many of the economic, social, political and technological benefits it brings could disappear.[275]

Google's statement is not completely correct. Google might like to operate in a world where protections on par with the American "Section 230" of the Communications Decency Act were universal. 47 U.S.C. §230 provides that; "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[276] Under the U.S. law, Google would not be liable as a publisher of the offending content.[277] The "notice and takedown" to which the Google statement refers concerns intellectual property rights, which apply to copyright.[278] Although some have argued that the Section 230 "notice and takedown" regime should apply to other content, such as anonymous libel, at present it does not.[279]

The EU E-Commerce Directive, on the other hand, provides that;

> *Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:*
>
> *(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or*

---

[275] "Official Google Blog: Serious threat to the web in Italy", (24 February 2010), online: <http://Googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html>.

[276] Communications Decency Act, *supra* note 269.

[277] The act does exempt some claims, such as state law intellectual property claims. Thus, in imagining the Italian case in an American context, it is possible that a state law right of publicity claim could have been plead that would not be protected by § 230. See, *Doe v. Friendfinder Network, Inc.* (2008), 540 2008 F Supp 2d 288.

[278] *Digital Millenium Copyright Act*, 1998, 17 USC 512 [*D.M.C.A. § 512*].

[279] Steven J Horowitz, "Defusing a Google Bomb" (2007) 117 Yale Law Journal Pocket Part 1, online: <http://yalelawjournal.org/the-yale-law-journal-pocket-part/intellectual-property/defusing-a-Google-bomb/>.

> *(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information*.[280]

This would have protected Google but for the important fact that data privacy matters are exempted. While this potentially imposes very difficult standards for providers in the EU, it also indicates the importance of privacy protections that this area of law would be specifically exempted from an otherwise blanket grant of immunity. The directives are also implemented in differing ways across the EU. Although the data controller could have been liable for a privacy violation in any EU country for the Italian video, it is conceivable Google could have instead been considered a mere "processor" and the originator of the video the controller. Also, it would have been possible in other EU countries to be found guilty but only liable for fines rather than imprisonment.

[280] Directive on Electronic Commerce, *supra* note 270 , section 14.

## 10. JURISDICTION

### 10.1 Introduction

Jurisdiction of the cloud has grown out of cases from the Internet era and earlier. In all contexts, this has evolved from a former rule of jurisdiction based on presence in a jurisdiction[281] to notions of constructive presence, or "minimum contacts."[282] International law followed a similar pattern, from jurisdiction based on presence to notions of constructive presence and later more permissive tests. Both systems are theoretically tempered by notions of reasonableness or "fair play and substantial justice" in the American terminology.[283] In determining their own competences, courts and legislatures are broadly tolerant of granting themselves extra-territorial jurisdiction, at least to make law and try cases. Limits on jurisdiction more often come from practical difficulties in enforcement. Enforcement must usually be based on some presence in a jurisdiction or enforcement by another nation under notions of comity, although sometimes a sort of soft enforcement power arises out of the desire by actors to be seen as respectable.[284] The upshot is that for many online actions there will be many jurisdictions with concurrent jurisdiction to make law or adjudicate cases; there may also be multiple states with the practical ability to enforce, although these states will be fewer than or at most coextensive with the states that have jurisdiction to legislate or adjudicate.

---

[281] It may sound awkward to refer to "jurisdiction within a jurisdiction." However, because of the multiple meanings of the word, it is not. Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge: Cambridge University Press, 2007) at 14.

[282] *International Shoe Co. v. Washington* (1945), 326 1945 US 310.

[283] *Ibid*.

[284] For example, in the controversies between Yahoo! and LICRA regarding the sale of Nazi memorabilia on Yahoo! auctions, Yahoo! seems to have complied with French demands regardless of whether they would have been enforceable in the United States. Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, *supra* note 246 Yahoo had little to gain in the court of public opinion from being seen as a purveyor of Nazi memorabilia in Europe.
.

"Most high-profile online businesses make a determined effort to comply with the laws of targeted states by, for example, having specially tailored sites which are compliant with local law, managed by local subsidiaries, even when evasion of local law would easily be possible." Kohl, *supra* note 281 at 208.

Article 2 Working Party, *Working Document on Determining the International Application of EU data protection law to personal data processing on the Internet by non-EU based web sites* (Brussels: Article 29 Working Party, 2002) at 15 (Notes that website operators may choose to comply with EU data protection practices even when not strictly necessary, "with a view to developing good business practice and to maintaining a good commercial image").

### 10.2 The end of Internet exceptionalism

A widely held popular misconception about jurisdiction and the Internet, or by extension, the cloud is that jurisdiction does not matter on the Internet. An early and poetic statement of this view came from former Grateful Dead lyricist and later Electronic Frontier Foundation co-founder John Perry Barlow in his Cyberspace Declaration of Independence;

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather….*
>
> *We are creating a world where anyone anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.*
>
> *Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here…*[285]

A similar view was expressed in more scholarly terms by Professors Johnson and Post that same year when they claimed that the Internet "radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules."[286] This special approach to the Internet was for a while also the official policy of the United States executive branch. In a groundbreaking policy paper, then President Bill Clinton and Vice President Al Gore spelled out an Internet policy calling for leadership and self-regulation by the private sector, a "minimalist" approach to regulation, and recognition of the "unique qualities of the Internet." It also conceptualized the Internet as somehow apart from the regular terrestrial rules of jurisdiction, stating; "Electronic commerce on the Internet should be facilitated on a global basis. The

---

[285] John Perry Barlow, "A Declaration of the Independence of Cyberspace", (8 February 1996), online: *Electronic Frontier Foundation* <https://projects.eff.org/~barlow/Declaration-Final.html>.

[286] David R Johnson & David G Post, "Law and Borders: The Rise of Law in Cyberspace" (1996) 48 Stan L Rev 1367, online: <http://cyber.law.harvard.edu/is02/readings/johnson-post.html>.

Internet is a global marketplace. The legal framework supporting commercial transactions should be consistent and predictable regardless of the jurisdiction in which a particular buyer and seller reside."[287]

Belief in such cyber-exceptionalism is no longer current among academics and practitioners, although it may still be popular among the general public, and some may still wish the Internet was indeed treated differently. If the Internet ever was a place outside space where borders were irrelevant, it certainly no longer is. The experience of the Internet varies from country to country, region to region, and now even among individuals. Google search results for sensitive topics will return very different results depending on the user's location, usually blocking out locally illegal content, such as Falun Gong in China, or potentially libelous content that would be acceptable elsewhere. The user experience of any number of websites and commercial services will vary by country as well. For example, Amazon's terms of service vary by country. Cloud music services like Pandora, Apple's iCloud, or Spotify may or may not be available depending on local law.[288] The providers generally have little difficulty in determining the location of the user. From time to time the assessment may be incorrect, and the savviest users may be able to fool them, for example by using proxy servers or other means.[289]

Years ago, Yahoo! unsuccessfully attempted to argue that it was powerless to adjust content for the French market. As the issue was new at the time, the French court set aside time for expert

---

[287] William J Clinton & Albert Gore, *The Framework for Global Electronic Commerce* (Washington, DC: The White House, 1997).

[288] When one attempts to access Pandora from Canada, a message apologizes that Pandora is only available in the United States. It goes on to state that it has determined the would be user is outside the United States based on his or her IP address and invites an email if this has been in error. An attempt to access Pandora from a mobile devise – perhaps because of space limitations – offers a much shorter explanation; "Pandora is not available in this country." "Pandora", (2012), online: *Pandora* <http://www.pandora.com>.

[289] Apple's iTunes store uses the credit card number of the user to determine nationality, so the iTunes store available to a given user follows the user when he or she travels. Canadians with access to a U.S. issued credit card (for example by borrowing a friend's) can gain access to the greater selection available in the U.S. iTunes store. Similarly, blocking based on a user's IP address can often be avoided by use of a "virtual private network". Most efforts to block content country-by-country, even if generally "good enough" can be circumvented by determined enough users.

testimony about the feasibility of doing so. The court heard the testimony of an entrepreneur who had created software designed to target advertising. Judge Gomez of the Tribunal de Grandes Instances found that new technologies could determine location accuracy at the country level with 99 percent accuracy.[290]

### 10.2.1 Imposing borders

Technologies that impose borders on the Internet have consistently increased in efficiency. Examples range from the benign to the extreme. Major League Baseball blocks Web-based broadcasts of games so as not to interfere with exclusive broadcast rights granted to certain television stations in local markets. Nations such as China, Iran, Saudi Arabia and Singapore engage in much more thorough censorship that are considered unacceptable by much of the world. While the user experience of the Internet varies from place to place, the infrastructure is also not free floating and immune to jurisdictional links. The same holds true for the cloud services that have grown up on the Internet. In the words of one prominent study, "While cloud computing is often talked of as something taking place in the distant obscure ether, in reality, as with all other forms of computing, it must ultimately make use of physical computers, with physical storage facilities, housed in physical structures."[291] The Internet is powered by physical computers and wires that must be located in actual places subject to one or more state's jurisdiction. This infrastructure is in turn owned by companies or people who are in turn subject to jurisdiction based on either physical presence or some other ties to any number of jurisdictions. Cloud computing has added another layer to the equation in that it adds more

[290] Goldsmith & Wu, *supra* note 244 , chapter 4 (Upon logging on to his American e-mail account in Paris and seeing American advertising, Houri is said to have had a realization that there was money to be made in geographically targeting ads. He founded a company, Infosplit that used IP addresses to allow advertisers to target ads based on the location of the user.).

[291] Hon, Hornle & Millard, *supra* note 7 at 2.

jurisdictional possibilities. Data that is outsourced to cloud providers across jurisdictional borders could provide additional jurisdictional hooks. [292]

### 10.2.2 Vulnerability based on location of infrastructure

Server location could also influence the practical possibility law enforcement intervention if the servers are targeted in an investigation. In a few cases this has also lead to so-called collateral legal damage as innocent clients of one data center have their operations interrupted during a search targeting another tenant of the same data center.[293] In the recent Megaupload.com case, the entire service was shut down as a criminal enterprise. Although at least some subscribers used the service for legal purposes, they too are in danger of losing their files. More confusingly, users of cloud services may or may not know the ultimate location of the data they are outsourcing.[294]

## 10.3 Types of jurisdiction

Jurisdiction is divided into three categories. These are legislative, adjudicative, and enforcement jurisdiction.[295] Legislative refers to competence of a nation's legislators to make rules about a given activity. Adjudicative jurisdiction is the power to try a specific case. Enforcement jurisdiction is the power to actually enforce a judgment. Enforcement jurisdiction is much more strictly limited than the other two; it is strictly territorial. "No State, its organs or individuals acting on its behalf can engage in any act to enforce its laws on the territory of

---

[292] In at least one New York case, the presence of a server in New York was a factor in helping the court find adjudicative jurisdiction for matters unrelated to the servers themselves. *Forward Foods Llc v. Next Proteins, Inc.* (2008), 2008 2008 NY Slip Op 52058.

[293] Kim Zetter, "FBI Defends Disruptive Raids on Texas Data Centers", (April 2009), online: *WIRED* <http://www.wired.com/threatlevel/2009/04/data-centers-ra/>; Verne G Kopytoff, "F.B.I. Seizes Web Servers, Knocking Sites Offline", *Bits Blog* (21 June 2011), online: <http://bits.blogs.nytimes.com/2011/06/21/f-b-i-seizes-web-servers-knocking-sites-offline/>.

[294] Hon, Hornle & Millard, *supra* note 7.

[295] *Restatement of the Foreign Relations Law of the United States, Third (1987)* (Philadelphia: American Law Institute, 1987), section 401.

another State; enforcement power is strictly territorial."[296] Even before the Internet, increased mobility in society was expanding the limits of adjudicative and legislative jurisdiction, which are often coextensive. Enforcement jurisdiction requires the cooperation of local courts. Judgments can be enforced through notions of comity or treaties providing for mutual recognition of judgments. Many restrictions exist that could cause foreign judgments not to be honoured. For example, judgments relating to public laws generally will not be enforced, nor will judgments against the public policy of the country from which enforcement is sought and only money judgments as opposed to orders to do or refrain from doing certain acts will be enforced, and then only under certain conditions that vary by situation.

### 10.3.1 Overlap of types of jurisdiction

Legislative jurisdiction and adjudicative jurisdiction frequently overlap. Adjudicative jurisdiction asks the question of whether a given court has authority over a given defendant. "In private actions, a court has the right to adjudicate a dispute if it has personal jurisdiction over the defendant."[297] *In rem* jurisdiction based on the location of property in the forum state can also serve as a basis for jurisdiction.[298] Personal jurisdiction can be assumed through actual or constructive presence in the forum state[299]. Choice of law (conflict of laws) corresponds to legislative jurisdiction. If a court has personal (adjudicative) jurisdiction in a private matter it will turn to its choice of law rules and apply either its own law or that of another state. In public (including criminal) matters there is no choice of law, so adjudicative and legislative

[296] Kohl, *supra* note 281 at 200.

[297] *Ibid* at 74.

[298] This has become important in the Internet context because of the location of the primary Domain Name Registry in the United States. IP addresses are also assigned regionally, with servers in the United States serving North America (including Canada) and the Caribbean. The U.S. government already exerts control based on domain names, as in the periodic "seizure" of websites, most recently "megaupload.com". The recently defeated SOPA/ PIPA legislation would have claimed jurisdiction based on either possibility. Whether or not it would comport with international law, U.S. authorities have the practical ability to "turn off" any website worldwide ending in .com or .net as well as the ability to "turn off" any website North America or the Caribbean. See, Michael Geist, "Michael Geist - SOPA: All Your Internets Belong to US", (16 November 2011), online: <http://www.michaelgeist.ca/content/view/6134/135/>.

[299] "State" here means jurisdiction, usually a nation. It could also mean a subdivision, such as a U.S. state.

jurisdiction will necessarily overlap. [300] Enforcement jurisdiction will exist in the forum state if the defendant is physically in the state. It could also rest in another state, in which case the forum state must rely on foreign recognition of its judgment.

In a bygone, less mobile age, enforcement jurisdiction was less likely to exist apart from enforcement jurisdiction. The former American rule was found in *Pennoyer v. Neff,* according to which, "The authority of every tribunal is necessarily restricted by the territorial limits of the State in which it is established. Any attempt to exercise authority beyond those limits would be deemed in every other forum, as has been said by this Court, an illegitimate assumption of power, and be resisted as mere abuse."[301] If physical presence were the only basis for jurisdiction, then enforcement would be less likely to be an issue unless the defendant was to leave the forum or otherwise hide. Choice of law (legislative jurisdiction) could be an issue, but courts have long been accustomed to dealing with this.

**10.4 Jurisdiction - Roots**

Courts have moved from strict limitations on jurisdiction based on geography to more expansive rules. The change in American law began with *International Shoe v. Washington*.[302] The U.S. Supreme Court, in *International Shoe* introduced a test of "minimum contacts." Under the *Shoe* approach, jurisdiction could be assumed provided an actor had minimum contacts with a state. The *International Shoe* approach had an important effect in bifurcating enforcement jurisdiction from the other types; "It meant that courts could sometimes exercise adjudicative jurisdiction even in the absence of enforcement jurisdiction."[303] The American test of when a court can exercise jurisdiction over a defendant not present in the forum jurisdiction was refined in a series of U.S. Supreme Court cases beginning with *Hanson v. Denckla*, which

[300] Kohl, *supra* note 281 at 17(see table).

[301] *Pennoyer v. Neff* (1878), 95 1878 US 714 at 720.

[303] Kohl, *supra* note 281 at 80.

introduced a requirement that the defendant "purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws." This requirement that a would-be defendant must purposefully avail itself of the benefits of doing business in the jurisdiction provides a basis for the later "targeting" approach to Internet jurisdiction. Other pre-Internet cases such as *Helicopteros Nacionales de Colombia v. Hall*[304] and *Asahi Metal Industry Co. v. Superior Court*[305] provide theoretical limitations on when courts can exercise jurisdiction. In *Asahi*, the U.S. Supreme Court held that the mere fact that items had been placed into the "stream of commerce" and later found their way to California where they had played a role in a tortious injury was not enough to subject the manufacturer to liability in a suit related to the defective products.[306] Concurring with the unanimous court, Justice O'Connor suggested a number of factors which might have helped satisfy constitutional limitations for a finding of jurisdiction. O'Connor noted a number of activities the petitioner (defendant) *did not do* that could have supported a holding that jurisdiction was appropriate. Justice O'Connor noted that since the company; "did not do business, have an office, agents, employees, or property, or advertise or solicit business in California, and since it did not create, control, or employ the distribution system that brought its assemblies to, or design them in anticipation of sales in, [the forum], it did not engage in any action to purposely avail itself of the [forum] market."[307] This can be seen as an antecedent to the targeting approach to Internet jurisdiction later employed in both the United States and Europe.

### 10.4.1 *Asahi* and *Helicopteros* for the digital age

It is easy to see how, following the *Asahi* reasoning, such factors as designing a website in a local language or accepting local currency or advertisements could be factors supporting

[304] *Helicopteros Nacionales de Colombia, SA v. Hall* (1984), 466 1984 US 408.

[305] *Asahi Metal Industry Co. v. Superior Court of Cal., Solano Cty.* (1987), 480 1987 US 102.

[306] The defective valves in question had changed hands a number of times before being incorporated into motorcycle tires sold in California. *Ibid*.

[307] *Ibid*.

jurisdiction. Some authors have already noted the similarity between an *Asahi*-type "stream of commerce" in physical goods and a stream of commerce in cloud services where many services in turn make use of other services in a sort of electronic stream of commerce.[308]

*Helicopteros* dealt with a suit unrelated to the defendant's rather tenuous previous contacts with the forum state, something like "general" jurisdiction in the American terminology. The Supreme Court held that for general jurisdiction to attach, the defendant's connection with the forum state must be "continuous and systematic." Undercutting these decisions is a concern for fairness, an approach Kohl calls "no pain, no gain." Even in cases where the *International Shoe* "minimum contacts" standard is met, it will often not be fair to subject a defendant to the forum state's jurisdiction. However, where a defendant has made a conscious decision to do business in the state, it will not be unfair to subject it to jurisdiction.

### 10.4.2 *Zippo*

In the Internet era, the American approach to jurisdiction in private law cases has transposed itself onto the Internet in important ways. The first is the sliding scale interactivity test developed in *Zippo v. Zippo Dot Com*.[309] In a widely cited decision, the United States Court for the Western District of Pennsylvania announced a "sliding scale" test of interactivity; the more interactive the site, the more likely it would be to subject the defendant to jurisdiction in the forum state. Zippo sued the owners of a website based in California, filing allegations of trademark infringement in Pennsylvania. All of the infringer's connections with Pennsylvania had been over the Internet. The court announced the "sliding scale" test. "A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction." However, at the other end of the spectrum lie

[308] Hon, Hornle & Millard, *supra* note 7; Allison MacDonald, "Youtubing Down the Stream of Commerce: Eliminating the Express Aiming Requirement for Personal Jurisdiction in User-Generated Internet Content Cases" (2009) 19 Alb LJ Sci & Tech 519, online: <http://www.albanylawjournal.org/articles/MacDonald_Format_YS.pdf>.

[309] *Zippo Mfg. Co. v. Zippo Dot Com, Inc.* (1997), 952 1997 F Supp 1119.

"situations where a defendant clearly does business over the Internet," in which case "jurisdiction is proper."[310] In the middle lie cases where the "interactive" web sites may or may not be commercial. In those cases exercise of jurisdiction is determined by "examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site." The interactive / passive test is perhaps the most widely cited test for Internet jurisdiction. However, it has been criticized, and it remains to be seen whether it will stand the test of time in an era when nearly all websites are "interactive." In light of technological change, the *Zippo* approach has been called "outdated and irrelevant."[311] It has nevertheless been employed in other countries, including Canada. [312]

### 10.4.3 *Calder v. Jones* and targeting

Nevertheless, the "current hodgepodge of case law is inconsistent, irrational and irreconcilable."[313] Other tests have been employed, including a sort of "effects" and/or targeting test in cases such as *Calder v. Jones*, a widely cited libel case.[314] Because California was the "focal point" of an allegedly libelous story available on the Internet, the publishers could be said to have "targeted" California, which they should have known would be the location where the injury was felt most. A plaintiff in a later case attempted to argue that defamation over the web could essentially lead to jurisdiction anywhere the injury would be felt (which would be anywhere the plaintiff had a reputation to defend.) The defendant had allegedly libeled a Virginia resident in a story published in Connecticut, but accessible online. The court looked at the totality of the situation and found that it was necessary "to look at

[310] *Ibid* at 1124.

[311] Michael A Geist, "Is There a There There? Towards Greater Certainty for Internet Jurisdiction" SSRN eLibrary, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=266932>.

[312] *Ibid* at 27.

[313] Kohl, *supra* note 281 at 85; Quoting, *Millennium Enterprises v. Millennium Music, LP* (1999), 33 1999 F Supp 2d 907 at 916.

[314] *Calder v. Jones* (1984), 465 1984 US 783.

whether the defendant has expressly aimed or directed its conduct toward the forum state." In the case at hand it had not.[315]

### 10.5 EU Rules on jurisdiction

The European Union has codified jurisdiction rules applicable to the web and cloud computing in rules such as the EC Jurisdiction Regulation generally and the Data Protection Directive for rules specifically related to data protection issues. Businesses domiciled in the EU can generally be sued in their home country.[316] Rules for "special jurisdiction" provide that a business can be sued in the place of the performance of a contract, unless otherwise agreed. Under Article 5(3), a tort victim can sue an EU domiciled defendant in the place or places where the "harmful event occurred." In defamation cases, this will be either the place of publication or the place where the plaintiff's reputation was harmed by the reading of the defamatory material. Countries will apply their own choice of law and choice of forum rules to cases involving non-EU defendants. These divisions are similar to the American concepts of jurisdiction in the place of a company's domicile or long-arm jurisdiction. However, while the provisions for "special jurisdiction" sound rather similar to American notions of "specific" long arm jurisdiction over defendants not domiciled in the forum state, there is no provision for "general" long arm jurisdiction.[317] This means that cloud providers in non-consumer contexts may be more effectively able to avoid jurisdiction in foreign courts for wrongs unrelated to their conduct in the forum state.

---

[315] *Young v. New Haven Advocate* (2002), 315 2002 F 3d 256.

[316] *Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*, 2000, 44/2001 [*EC 44/2000*].

[317] See, *Gorman v. Ameritrade Holding Corp.* (2002), 293 2002 F 3d 506..

Because Ameritrade, a foreign corporation, had "continuous and systematic" contacts with DC, it was "doing business" within the state and was subject to general jurisdiction. "District of Columbia law also permits courts to exercise "general jurisdiction" over a foreign corporation as to claims *not arising from the corporation's conduct in the District*, if the corporation is "doing business" in the District." (emphasis added.)

The European Court of Justice has also addressed questions of when a website is "directed to" another state, notably in the joined case of *Pammer/Alpenhof*.[318] In that decision, it was held that to be said to be "directed to" a member state a commercial website "must have manifested its intention to establish commercial relations with consumers from one or more other Member States including that of the consumer's domicile." A six-point list of factors to consider is similar to the factors Justice O'Connor noted in the *Asahi* concurrence.[319] However, it should be noted that directing is only relevant for some purposes, such as jurisdiction over consumer contracts.[320]

### 10.5.1 Consumer protections

Consumers receive protection under Article 15(1)(c) and are able to sue in their home jurisdiction whenever the defendant has "directed" activities at the plaintiff's home. The liberal interpretation courts have given this means that consumers will usually have the right to sue in their home jurisdictions.[321] Pre-dispute forum selection clauses are unenforceable.[322] In the

---

[318] Joined Cases C-585/08 and C-144/09, *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09)*, judgment 7 December 2010

[319] "The following matters, the list of which is not exhaustive, are capable of constituting evidence from which it may be concluded that the trader's activity is directed to the Member State of the consumer's domicile, namely the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that other language, mention of telephone numbers with an international code, outlay of expenditure on an Internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.

On the other hand, the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled is insufficient. The same is true of mention of an email address and of other contact details, or of use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established." *Id.*

Online <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62008J0585:EN:HTML>

*See also,* Hon, Hornle & Millard, *supra* note 7 at 36.

[320] EC 44/2000, *supra* note 316.

[321] Reference to Kohl – since existence of a consumer contract is taken as evidence of "directing" toward the consumer's home jurisdiction, "directing" will almost always be found when there is a consumer contract.

[322] Contrast to, *Carnival Cruise Lines, Inc. v. Shute* (1991), 499 1991 US 585..

United States, cloud providers are typically able to insulate themselves from suits outside their home jurisdiction through click-wrapped choice of forum and choice of law agreements.[323] Kohl suggest the EU "directing" requirement is similar to American notions of "targeting" to establish jurisdiction, but notes that EU authorities have rejected comparisons that could import American experience to the interpretation of EU law. Providers, including American companies, have complained of the inefficiency of having to be ready to defend suits in every EU jurisdiction.[324]

### 10.5.2 Data protection jurisdiction

Jurisdictional rules for data protection issues are spelled out in the Data Protection Directive. Controllers located outside the EU will be subject to jurisdiction in any territory where they gather personal data by means of "equipment", a definition that includes "cookies" installed on users' computers. Thus, if a foreign service were to install browser cookies and collect information from Europe, it could fall under the purview EU data protection law, even if it had not otherwise directed its activities at Europe. Thus, a service with no EU office could be subject to jurisdiction anywhere in the EU, provided enforcement could be obtained. A provider with an "establishment" in the EU will be subject to jurisdiction in the country or countries in which it has such an establishment.[325] Processors will be subject to the law in which they operate. However, the laws governing processors are not the general data control regime, but rather an obligation to act only on the orders of the controller and an undertaking to practice sound security precautions. Member state laws require controllers to see that processors operating on their behalf, implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration,

[323] See, ProCD, Inc. v. Zeidenberg, *supra* note 134 for U.S. treatment of "click-wrap" agreements).

[324] This does not discourage cloud providers from attempting to limit jurisdictional exposure by choice of law and choice of forum clauses in EU consumer contracts, even in many cases where they may not be enforceable. Bradshaw, Millard & Walden, *supra* note 77.

[325] For explanation of applicable rules on jurisdiction, see, Article 29 Working Party, *Opinion 8/2010 on applicable law* (Brussels: Article 29 Working Party, 2010).

unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."[326]

### 10.5.3 Continuing incentives to jurisdiction shop

Although the DPD was intended to harmonise EU law relating to data collection and processing, significant differences exist, both in the implementation into local law and in the attitude of local Data Protection Authorities. The attitudes and perceived business-friendliness of various DPAs varies as well, with the German authorities generally seen as the toughest, and the Irish and UK seen as the most business-friendly. Since companies that collect data but do not have an EU "establishment" can potentially be subject to jurisdiction anywhere in the EU, they may find a strategic advantage in having an EU establishment in a friendly jurisdiction.[327] Frequently, this is Ireland, sometimes to the dismay of other data protection authorities as the Irish DPA is reputed to have a light touch.[328] However, having an "establishment" elsewhere can lead also to jurisdiction in multiple nations. For example, Google's offices in Italy were held to be an establishment for purposes of data protection jurisdiction in the case involving its subsidiary Youtube and that saw some of its executives receive suspended prison sentences. Unfortunately for Google, Italy had both a local implementation of the Data Protection Directive that permits criminal penalties as well as an enthusiastic prosecutor. Facebook, meanwhile, limits its European exposure to its office in Ireland, making Irish authorities the lead regulators for the social networking site. Thus, when the "Europe-vs.-Facebook" project started by Austrian law student Max Schrems started urging Facebook users to demand the social networking giant divulge the information it held on them, it was to the Irish office that the demands were sent. Likewise, it was the Irish DPA that investigates of Facebook's practices.[329]

---

[326] 95/46/EC, *supra* note 85 , section 17.1 .

[327] This could also be a functional necessity to have servers close to markets, increase speed, reduce latency, etc.

[328] Aoife White, "Can Ireland's Regulators Stand Up for Internet Privacy?", *BusinessWeek: Magazine* (9 February 2012), online: <http://www.businessweek.com/magazine/can-irelands-regulators-stand-up-for-Internet-privacy-02092012.html>.

[329] *Report of Data Protection Audit of Facebook Ireland* (Dublin: Data Protection Commission, Ireland, 2011).

### 10.6. Broad scope

In non-contractual matters, most countries will assume broad jurisdiction over activity which causes a perceived harm in the forum state. For example, as Judge Gomez opined in the French Yahoo! case, "the harm is suffered in France, our jurisdiction is therefore competent.[330] In most private law cases, including defamation cases, jurisdiction can be assumed in the place where harm is felt. For the Internet, a seminal case in this vein is the Australian case of *Gutnick v. Dow Jones.*[331] The Plaintiff, a resident of Australia, suffered harm in Australia when Dow Jones published allegations of illegal activity in *Barron's*, a financial magazine published in the United States. *Barron's* also had several thousand web subscribers in Australia who were able to access the story online. The choice of forum and law were important to the case as the plaintiff would have had to overcome the defendant-friendly protections of the First Amendment as interpreted in *New York Times v. Sullivan* had he sued in the United States. Nevertheless, Gutnick was able to sue in Australia and secured a retraction and settlement from the defendant.

Broad assertions of jurisdiction in private law matters are generally tolerated in international law. Indeed, it has been said that "[t]here is no effective or established customary international law that regulates personal jurisdiction."[332] Nevertheless, some courts have declined to exercise jurisdiction in cases with trivial connections to the forum state. For example, in the trademark case *Bonnier Media Ltd. V. Greg Lloyd Smith*, a Scottish court declined jurisdiction, noting that "the overwhelming majority of websites will be of no interest whatsoever in more

[330] Association Union des Etudiants Juifs de France v. Yahoo! Inc., *supra* note 245.

[331] *Dow Jones and Company Inc v Gutnick*, 2002 56 (available on http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html).

[332] Jack L Goldsmith & University of Chicago Law School, "Against cyberanarchy" (1998) 65 U Chi L Rev 1199, online: <http://groups.csail.mit.edu/mac/classes/6.805/articles/goldsmith-against-cyberanarchy.html>.

than a single country or a small group of countries."[333] However, courts have tolerated seemingly trivial connections with the forum state as a basis for jurisdiction.[334] According to one commentator "many, not to say most, states' private international law rules do in fact provide for jurisdictional claims over, and the application of the state's law to, any website that can be accessed in their respective territories, in relation to a wide range of legal matters."[335]

### 10.7. Overlap

The end result of the rather liberal worldwide approach to jurisdiction subjects providers to potential claims in numerous states. Depending on the jurisdiction in question companies can be subjected adjudicative jurisdiction either for acts or omissions related to their activities or for any activities at all in a state in which they have pervasive enough contacts. Risk management techniques can include avoiding certain jurisdictions or contracting out of liability. The varying availability of personal-use cloud services attests to this. For example, the music and movies services Hulu, Netflix, Pandora, Spotify, and Apple's iCloud all vary in availability by country.[336] Technological attempts to limit jurisdictional risk probably need not be airtight. For example, determined users can usually find some way around.[337] However, they must be reasonably good. Sham attempts generally will not succeed. For example, icravetv streamed American and Canadian television over the Internet from Canada in 1999 and 2000. The site claimed not to target Americans. Users were required to supply a Canadian telephone area code and click a box to "prove" that they were in Canada. In reality, most users were probably

---

[333] *Bonnier Media Ltd. v. Greg Lloyd Smith and Kestrel Trading Corporation* (Court of Session, Soctland, 1 July 2002), www.scotcourts.gov.uk/opinions/dru2606.html)

[334] For example:

*Harrods Ltd. v. Dow Jones & Co. Inc.,* [2003] EWHC 1162 (QB) (ten subscribers in the UK and a handful or website visitors)

*Kitkufe v. Olaya Ltd.* (two website visitors in Canada)

[335] Dan Jerker B. Svantesson, *Private International Law and the Internet* (Kluwer Law International 2007) 1

[336] All of these also involve music licensing deals which vary by country.

[337] How-to sites such as the following abound; "How to watch Netflix outside the U.S." http://vpnfreedom.com/netflix/how-to-watch-netflix-outside-the-us/

American. Many simply supplied 416, the Toronto area code that was visible on the site. The American court called this a "meaningless screen."[338] In the reverse situation, it was once common for American websites to ask for an American zip code (postal code) to prove residence in the U.S. The most popular was said to have been 90210, widely known because of the "Beverley Hills 90210" television show.

### 10.8. Special concerns with public law

Much of the law relating to cloud computing and the Internet is public law, meaning the un-waivable law governing the relationship of the state to its citizens, including criminal law. Examples include competition law, tax law, and all criminal law. Unlike in private law, parties never have a choice as what public law will govern them. Also, in public law matters, courts will never address choice of law issues; if a court has adjudicative jurisdiction, meaning personal jurisdiction over both parties, it will apply its own law. The public / private split also matters in the enforcement stage because nations are much less likely to enforce their neighbours' public law judgments. to a "taboo" against foreign enforcement of public law judgments.[339] Some matters likely to be relevant in cloud computing, notably data protection law, will be difficult to categorize as public or private law.[340]

#### 10.8.1 A multitude of potential basis for jurisdiction

Presence in the territory of a state – the territoriality principle – was long the standard for jurisdiction in public law. A number of theories now take their places alongside the territoriality principle as bases for jurisdiction. The "effects doctrine" may be either an extension of the territoriality principle or a new basis altogether.[341] With varying degrees of controversy, bases

---

[338] http://euro.ecom.cmu.edu/program/law/08-732/Jurisdiction/icravetvcomplaint.pdf (para 44)

[339] Kohl, *supra* note 281 at 230 – 238.

[340] Kuner, *supra* note 88 at 181.

[341] Kohl emphasises the continuity of its growth from the territoriality principle. Kuner lists the effects doctrine as its own basis for jurisdiction. Kuner, Christopher. "Data Protection Law and International Jurisdiction on the Internet (Part 1)" (2010) 18:2 IJLIT 176

for extraterritorial jurisdiction include territoriality, effects, personality, and protection of the state (the protective principle). The nationality of either an offender or a victim can serve as a jurisdictional hook, although this is sometimes controversial.[342] The protective principal allows states to assert jurisdiction over a limited class of wrongs targeting the state itself, such as terrorism.

### 10.8.2 Constructive presence

International jurisdictional in public law cases has undergone a transformation from being completely territory-dependent to one much more permissive of exercises of jurisdiction in cases where the act did not take place in the territory of the forum state or the defendant is not domiciled or found in the forum state. The *Lotus* case is often cited as the beginning of the end of the "pure" territoriality restriction. In that case, a French ship accidentally collided with a Turkish ship causing death and destruction of property. Turkey sought to exercise jurisdiction over the sailors responsible for the accident. The Permanent Court of International Justice held that under concept of "constructive presence" a state can punish a defendant not in the jurisdiction when a crime has an effect within the forum state, in this case the Turkish flagged ship. Kohl notes that the Permanent Court was unclear about whether it was the existence of "effects" in the jurisdiction versus whether it was necessary that a constituent element of the crime had taken place in the forum jurisdiction.[343]

## 10.9 Jurisdiction based on effects

At first, "effects" based jurisdiction was believed to be limited to cases where a *physical* effect (such as deaths or damage) was felt within the forum state. Beginning in the 1940s and gathering pace through the 1970s and 1980s, the United States would embark on a program of

[342] Kuner, *supra* note 88.

[343] Accused can be deemed to have committed a crime in the forum state if "one of the the constituent elements of the offense, and more especially its effects have taken place there." *The Case of the S Lotus (France v. Turkey)* (1927) PCIJ Reports, Series A. No 10, 23.

extra-territorial enforcement of its antitrust laws that would defy traditional understanding of this requirement.[344] This was controversial chiefly because the effects of antitrust violations, although real to investors, were not in any sense physical. While controversial, this did pave the way for more liberal worldwide rules for extraterritorial jurisdiction;

*The real problem with the US expansion of the effects doctrine is the intangibility of the effects. If there is no requirement that the effect be physical, the number of States potentially entitled to claim jurisdiction on the basis of the economic effects of foreign activity spirals significantly*.[345]

The inclusive U.S. approach never gained wide acceptance before the advent of the Internet. However, echoes of the approach can be seen in the willingness of states to claim jurisdiction based on the intangible effects of websites, as in the French Yahoo! decision.[346] Some limitation has been placed on the extra-territorial reach of public law by notions of reasonableness. For example, states should decline jurisdiction when the "exercise of such jurisdiction is unreasonable."[347] However, this limitation seems to be limited such that if a country perceives a threat to its own interests it will find jurisdiction "reasonable." A limitation on reasonable exercise of jurisdiction might exist if, for example, a small number of technically savvy users of a cloud service from a country the service attempted to block managed to circumvent protections designed to keep them out.

### 10.9.1 Broad scope of possible effects-based jurisdiction

Effects, on the other hand, can include any number of wrongs sought to be prevented, such as the viewing of Nazi memorabilia in France, online gambling, loss of privacy, mishandling of personal data, or corrosion of faith in the financial markets. For example, New South Wales (Australia) states that a person has committed a crime within the state if "the offense is

[344] Such as *U.S. v. Aluminium Company of America* 148 F 2d 416 (1945

[345] Kohl, *supra* note 281 at 92.

[346] "Attendu que le dommage étant subi en France, notre juridiction est donc compétente pour connaître du présent litige." Association Union des Etudiants Juifs de France v. Yahoo! Inc., *supra* note 245.

[347] Restatement (Third) of Foreign Relations Law (1986) Sec. 403(1).

committed wholly outside the state, but the offense has an affect within the state." Australia will also assert its federal securities laws over any securities offering "received in Australia". Since any securities offering posted on the Internet is potentially viewable in Australia, the scope of this could be sweeping. Likewise in the offshore gambling case of *People v. World Interactive Gaming Corp.,*[348] New York found that the legality of the gambling activity in Antigua, where the website was based, was irrelevant, especially since the website appeared to have targeted New York;

> *A computer server cannot be permitted to function as a shield against liability, particularly in this case where respondents actively targeted New York as the location where they conducted many of their allegedly illegal activities*.[349]

The limitations imposed by the targeting requirement are scant as well. As in defamation cases where jurisdiction has been asserted despite a paucity of actual readers in the forum state, the level of "effect" necessary in the forum state is small. For example, a French pornographer living in England was prosecuted in England for a web site there was no evidence anyone in England ever visited.[350] A German born Australian citizen resident in Australia was successfully prosecuted for a Holocaust denial website – in English – despite no evidence that anyone besides the police had ever visited the site from Germany.[351] If a state sees its perceived interest threatened it will be able to find some basis for jurisdiction. What limitations do exist are a matter of disagreement among states, which "have been creative in finding justifications for the assertion of legislative jurisdiction under a variety of legal grounds."[352] Bases for jurisdiction over websites generally will provide grounds for jurisdiction over cloud services, which are often accessed through a website and are highly interactive.

---

[348] *People v. World Gaming Corp* (1999), 185 1999 Misc 2d 852.

[349] *Ibid*.

[350] *Perrin, R v [2002] EWCA Crim 747 (22nd March, 2002)*, 2002 (available on http://www.bailii.org/ew/cases/EWCA/Crim/2002/747.html).

[351] *Toben* (2001), 8 2001 Neu Juristische Wochenschrift 624; See also commentary in, German Law Journal, "Federal Court of Justice (BGH) Convicts Foreigner for Internet Posted Incitement to Racial Hatred" (2001) 2 German Law Journal, online: <http://www.germanlawjournal.com/article.php?id=67>; See also commentary in, Kohl, *supra* note 281.

[352] Kuner, *supra* note 88 at 11.

### 10.10 Enforcement power as the practical limitation on jurisdiction

In most of the above cases, one element besides a perceived wrong existed – the ability to enforce the judgment. Even in *Toben*, involving the publisher of the Holocaust denial website, the defendant was charged only when he was in custody on related charges of distributing similar German-language printed material in Germany. According to Goldsmith, "the true scope and power of a Nation's regulation is measured by its enforcement jurisdiction, not its prescriptive jurisdiction."[353] States typically do not waste their credibility or their resources pursuing judgments they will not be able to enforce.

> *When in possession of enforcement power, States tend to exercise adjudicative jurisdiction (especially in respect of online activity which is contrary to their fundamental moral and cultural values) not only when the effects on the territory are intended and substantial, but upon the most tenuous basis. But the strict limits of enforcement jurisdiction to some extent temper the blanket application of the 'crude' effects doctrine*.[354]

This might sound like a recipe for anarchy in a sort of rush to the bottom. Couldn't all publishers of potentially libelous material do so from the United States while all gambling websites could locate themselves in the UK or some Caribbean island where Internet gambling is perfectly legal? Couldn't some country set itself up as a sort of haven for dodgy practices such as the recently-shut down Megaupload "cloud locker" program that served as a base for copyright infringement? Couldn't cloud services in a sort of "data haven" target EU consumers depriving them of the consumer and privacy protections guaranteed under EU law?

A number of practical protections exist. States have available to them a variety of ways to enact their own policies over what is available via the Internet within their territory. To the extent that foreign cooperation is available, they can enforce their judgments and policies

---

[353] Jack Goldsmith, 'Unilateral Regulation of the Internet: A Modest Defence' (2000) 11 European Journal of International Law 135, 139,

[354] Kohl, *supra* note 281 at 109.

internationally. Even in where international cooperation is not available, a great deal of regulation can be accomplished through intermediaries. A website or cloud service does not make its way to the end user unaided. For example, local Internet service providers (ISPs) can be banned from carrying certain websites. New Zealand does not directly outlaw Internet gambling, but instead has outlawed promotion, advertisement, or financing of gambling operations from New Zealand.[355] The ban also applies to search engines or advertisers that could indirectly promote gambling services. Various governments have also targeted financial intermediaries, including successful American efforts to dry up funds for Antiguan gambling and untaxed cigarette sales.[356]

More recently, American authorities used persuasive power of dubious legal authority to make the anti-secrecy website Wikileaks such a hot potato that many financial intermediaries will no longer work with it.[357] Goldsmith and Wu devote a chapter in their book, *Who Controls the Internet?* to describing the ways in which governments control the Internet within their territories.[358] In the chain from the website or cloud service provider, to ISP, to end user and financial intermediaries, only one link need be within the control of the government in question.[359] States such as Saudi Arabia, Iran, and China that are not shy about censorship can go much further, imposing tighter controls though national telecoms, controls at borders, or even sophisticated internal snooping.[360] While the most extreme cases can be objectionable,

---

[355] Section 4 of the Gambling Act 2003. See discussion in Kohl, Uta. *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge: Cambridge University Press, 2007), 174.

[356] Goldsmith & Wu, *supra* note 244 at 76 – 77, 172 – 173.

[357] http://www.guardian.co.uk/commentisfree/2011/oct/24/bankers-wikileaks-free-speech

[358] Goldsmith & Wu, *supra* note 244 Chapter 5 "How Governments Rule the Net".

[359] *Ibid*.

[360] *Ibid*. See Chapter 6 devoted to Chinese Internet controls

See also, "Mapping Local Internet Control - GeoMap Visualization Demo", (2012), online: *Berkman Center for Internet & Society at Harvard University* <http://cyber.law.harvard.edu/netmaps/geo_map_home.php>; For information on control by "deep packet inspection", see, Ben Wagner, *Deep Packet Inspection and Internet Censorship: International Convergence on an "Integrated Technology of Control"* (Global Voices Advocacy) online, <http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandInternet-censorship2.pdf >; Ronald Deibert, *Access Denied: The Practice and Policy of Global Internet Filtering* (MIT Press,

states do have a practical ability, for the most part, to control much or most of what content or services are available within their borders.

### 10.11 The practical option to avoid certain countries

As noted above, "most high-profile online businesses make a determined effort to comply with the laws of targeted states."[361] This leaves open the possibility of not targeting some states. The varying availability of cloud music and entertainment services noted above, provide examples. In contrast, Dow Jones could be said to have chosen to do business in the Australian market, where it had subscribers, offices, and property. After the *Gutnick* decision it could also have decided that the Australian market was too risky and withdrawn from it, which it has not done. Some publishers or web services might be able to avoid either adjudicative or at least enforcement jurisdiction by avoiding problem countries. Sometimes, although a forum country might assert jurisdiction it might not have the practical ability to enforce it. This occurred in the Yahoo! case, where the ongoing fine against Yahoo! would have faced various issues in the U.S, including its possible objectionability on first amendment grounds and whether it was an example of public or private law. [362]

### 10.12 An illustration - Twitter

Twitter, the popular "micro-blogging" service provides an illustration of the conundrums faced by growing cloud services. Although they could theoretically avoid the problems of compliance in multiple countries, doing so would destroy the benefits of a global Internet and global cloud services. Companies are subject to adjudicatory and enforcement jurisdiction – meaning the

---

2008); John G Palfrey, OpenNet Initiative & Rafal Rohozinski, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (MIT Press, 2010).

[361] Kohl, *supra* note 281.

[362] Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, *supra* note 246(The district court concluded that "the First Amendment precludes enforcement within the United States"). Yahoo! Inc. v. La Ligue Contre Le Racisme, *supra* note 246(However, the 9th Circuit reversed, holding the case was not ripe. The 9th Circuit opinion thus did not address the First Amendment issues).

ability of a nation's courts to try cases *and* actually enforce them – in at least the countries in which they have offices, employees, or assets. Twitter has never attained the number of users of, for example, Facebook, but it is a favourite among newsmakers, news reporters and other influential people. It hosts its data in its own servers in New York City and San Francisco, although it is building an impressive, custom built data center in Utah. It has offices and employees in the United States, the UK, and Ireland.

The service won broad acclaim for "beta-testing a spine" and resisting efforts by the U.S. government to obtain information about Twitter users associated with the Wikileaks anti-secrecy site.[363] Twitter fought first against a gag order not to disclose the subpoena and then the subpoena itself. Although the service succeeded in publicizing the subpoena and its efforts against it, it eventually lost on the merits. The U.S. government was successful in compelling the disclosure of account information, such as IP addresses associated with Twitter accounts.[364] Twitter, nevertheless, gained aplomb for fighting the request. However, because of the "third party doctrine" of U.S. Fourth Amendment law, Twitter was ultimately powerless against a subpoena under the Stored Communications Act.[365] One aspect of the case that was never in doubt was that Twitter was subject to the jurisdiction of the U.S. federal court in Virginia. Ignoring the order was simply not an option. In the most extreme scenario, federal agents would have been able to compel compliance by physically searching Twitter's premises, fining

[363] Ryan Singel, "Twitter's Response to WikiLeaks Subpoena Should Be the Industry Standard", *Wiredcom* (10 January 2011), online: <http://www.wired.com/threatlevel/2011/01/twitter/>.

[364] The subpoena did not deal with *content* information such as the actual content of user tweets. Under the Stored Communications Act, content information enjoys higher levels of protection that account information. See, *Electronic Communications Privacy Act*, 1986, 18 USC 2701 et seq [*Electronic Communications Privacy Act*]..

[365] Some Web commentary mistakenly focused on Twitter's terms and conditions, including the fact that the users had signed up under more protective terms and conditions than those existing at the time of the subpoena. *See*, Christopher Soghoian, "Twitter's privacy policy and the Wikileaks case",, online: <http://paranoia.dubfire.net/2011/11/twitters-privacy-policy-and-wikileaks.html>.. Twitter's policies were actually irrelevant because users had entrusted their information to a third party. See, *In re Application of the United States of America for an order pursuant to 18 U.S.C. 2703(d) (memorandum opinion)*, 2011 1:11-DM-3 (available on http://www.aclu.org/files/assets/twitter_mem_op_11.10.2011.pdf) at 28.

the company, or confining employees for contempt of court, none of which powers would be guaranteed if the company was located outside the United States.

### 10.12.1 Twitter – Initial resistance to authority

Also in 2011, Twitter gained attention by being the conduit through which a "super-injunction" was widely flouted in the United Kingdom. "Super injunctions" are a measure under UK law by which a court can order that certain speech be restrained. Additionally – and this is the "super" part – it becomes illegal to even mention the existence of the injunction.[366] The injunctions are unpopular in the UK and would almost certainly be illegal as a prior restraint on speech in the United States.[367] Celebrities, including a football star, had obtained an injunction against being named as a suspected adulterer.[368] In 2011, UK Twitter users began flouting these super injunctions on Twitter.[369] In the United States, Twitter would benefit from "section 230" immunity under the Digital Millennium Copyright Act[370] The footballer later commenced action against Twitter and obtained a judgment ordering it to cease future publications and to assist in unmasking users who violated the injunction. Commentators noted that enforcing the order against Twitter at home in California would be difficult as Twitter had no assets or offices in the UK. "Twitter will probably just ignore it and consider it to be offensive to their first amendment rights**,"** as one London lawyer told Bloomberg News.[371] The UK plaintiffs would find themselves in a situation similar to the French plaintiffs in the Yahoo! case, free to seek enforcement in

---

[366] Lord Neuberger, *Report of the Committee on Super-Injunctions: Super-Injunctions, Anonymised Injunctions and Open Justice* (London: Judiciary of England and Wales, 2011).

[367] *Doe v. Ashcroft* (2004), 334 2004 F Supp 2d 471 at 495("National Security Letter" gag orders as unconstitutional prior restraint)."

[368] *CTB v News Group Newspapers Ltd & Anor [2011] EWHC 1232 (QB)*, 2011 (available on http://www.bailii.org/ew/cases/EWHC/QB/2011/1232.html).

[369] Katy Barnett, "Twitter Undoes UK Super Injunctions «", *The Fortnightly Review of IP & Media Law* (2 June 2011), online: <http://fortnightlyreview.info/2011/06/02/twitter-undoes-uk-super-injunctions/>.

[370] Communications Decency Act, *supra* note 269.

[371] Lindsay Fortado & James Lumley, "Twitter Inc., Unknown Posters Sued by Athlete Known as 'CTB' at U.K. Court", *Bloomberg* (20 May 2011), online: <http://www.bloomberg.com/news/2011-05-20/twitter-inc-unknown-posters-sued-by-athlete-known-as-ctb-at-u-k-court.html>.

California but facing hurdles. Twitter would be able to argue that its conduct was protected by Section 230 of the Communications Decency Act and also that the UK order was repugnant to the First Amendment of the U.S. Constitution. Had Twitter defended in the UK it could have tested the "mere conduit" defense under the UK implementation of the EU E-Commerce Directive.[372]

### 10.12.2 Coming of age – tailoring behaviour to local law

In a sort of "growing pains" development for Twitter, it recently announced that it will institute new systems that will enable it to comply with local law. For the first time, Twitter will appear differently in different countries. This is because Twitter will be implementing a system to comply with lawful orders throughout the world by removing tweets that violate local law. As the Electronic Frontier Foundation explained Twitter's new policies;

> *Twitter's increasing need to remove content comes as a byproduct of its growth into new countries, with different laws that they must follow or risk that their local employees will be arrested or held in contempt, or similar sanctions. By opening offices and moving employees into other countries, Twitter increases the risks to its commitment to freedom of expression. Like all companies (and all people) Twitter is bound by the laws of the countries in which it operates, which results both in more laws to comply with and also laws that inevitably contradict one another. Twitter could have reduced its need to be the instrument of government censorship by keeping its assets and personnel within the borders of the United States, where legal protections exist like CDA 230 and the DMCA safe harbors…* [373]

Although Twitter's announcement provoked "@outrage" from some observers,[374] the Electronic Frontier Foundation (EFF) actually praised Twitter's policy, noting; "*All* of the other

---

[372] The "mere conduit" defense would have provided some protection similar to 47 U.S.C. § 230 available in the United States.

[373] Eva Galperin, "What Does Twitter's Country-by-Country Takedown System Mean for Freedom of Expression?", (27 January 2012), online: *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2012/01/what-does-twitter%E2%80%99s-country-country-takedown-system-mean-freedom-expression>.

[374] Somini Sengupta, "When Twitter Blocks Tweets, It's #Outrage", *The New York Times* (27 January 2012), online: <http://www.nytimes.com/2012/01/28/technology/when-twitter-blocks-tweets-its-outrage.html>.

commercial platforms that we're aware of remove content, at a minimum, in response to valid court orders."[375] Furthermore, the Twitter plan is transparent in that users will be aware when content is blocked. It is also the least restrictive option possible to comply with orders from around the world; content that is blocked in one country will still be visible in other countries. Twitter has since stated that in the future they will cooperate with a lawful order from the UK such as the "super injunction" orders of mid-2011.[376] In the interim, Twitter has also opened offices in the UK. The EFF noted how the growth of Twitter's geographic footprint corresponded to the growth of its legal exposure, including at least the places where Twitter had offices and employees. At the time, this included the UK, Ireland, Japan, and Germany. [377]

### 10.13 Jurisdiction and the cloud meet

Twitter's growth and the policy changes it necessitated illustrates the fact that no website or cloud service can exist outside the jurisdiction of states. The popular myth of the Internet as somehow outside territorial control is certainly no longer true, if it ever was. An extreme example of this is provided by the experience of "Sealand", the proto-state of an eccentric British man who claimed a decrepit air defence platform in the Atlantic as a sovereign nation. Roy Bates, the putative head of government and state, sought to turn Sealand into a "data haven" for Internet activities unwelcome elsewhere – presumably things like gambling or pornography. The plan failed, mostly for lack of intermediaries, especially banks, willing to cooperate.[378] More recent attacks against intermediaries include the shutdown of Antiguan gambling sites and the evisceration of Wikileaks. Governments also have the final backstop of

[375] Galperin, *supra* note 373 (emphasis in original).

[376] Editors, "Twitter to block super injunction tweets in Britain", *TNT Magazine* (31 January 2012), online: <http://www.tntmagazine.com/news/games/twitter-to-block-super-injunction-tweets-in-britain>.

[377] Galperin, *supra* note 373.

[378] Goldsmith & Wu, *supra* note 244 at 65–85.

blocking certain services within their borders, although not all have the determination or desire to follow in the steps of Iran or China.[379]

Companies that wish to progress beyond local scale must be mindful of jurisdictional exposure to an increasing number of countries. While staying local may be an option, that in itself would deprive the world of the benefits of "jurisdictional indifference" noted earlier in this paper. Twitter's new policy to provide for country-by-county blocking of content represents the reality that borders are now being built into the design of cloud systems. Cloud infrastructure – the actual wires and data centers – must be built somewhere, and the laws of the countries in which it will be built will of course be a factor in deciding where to locate it. For example, if a given country had ideal conditions – proximity to markets, cheap power, ample fibre-optic cable, etc. – but was ruled by a capricious government prone to snooping, high and unpredictable taxation, and a lack of respect for intellectual property rights, it would possibly take itself out of the running as a location for a company's next data center despite its appealing qualities. Companies can of course differ in their assessments; while Google claims Sweden's snooping law renders it unfit as a data center location, Facebook, drawn chiefly by cheap and abundant power has decided to make Sweden the home of its first data center outside the United States.[380]

### 10.13.1 Risks from jurisdictional exposure

Whatever the case may be, the cloud has changed the equation by sometimes radically increasing the number of jurisdictional contacts websites and services have. Cloud services

---

[379] However, even among democracies, various proposals for blocking appear frequently. The U.S. government already blocks sites to stop piracy and would have greatly increased its powers to do so under either the Stop Online Piracy Act or it's sibling the Protect Intellectual Property Act.

Belgium sought to force ISPs to preemptively filter content to prevent piracy, but was rebuked by the Court of Justice for the European Union. *Judgment in Case C-70/10: Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Court of Justice of the European Union, 2011) online, <http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126en.pdf>.

[380] Leach, *supra* note 52; Horn, *supra* note 52.

must now consider the country of residence of their users as well as their headquarters and infrastructure. Most of the pre-cloud Internet jurisdiction cases seem to assume that the company's servers or data centers were located at the place of the company's headquarters.[381] Not only does jurisdictional exposure increase, but predictability and control decrease. Companies might not know where their data is stored. While technologists might like to proclaim that the locations of servers are irrelevant, there is no such principle among lawyers. Cloud data center providers have been targeted in efforts targeting their clients ("tenants"). In at least two such cases in the United States investigations targeting one client of a cloud provider caused damage or at least inconvenience to other innocent users.[382] In the recent case of Megaupload, all users of the service have been left without their data. While it is probable that a significant portion of Megaupload's users were "pirates" engaged in illegal file-sharing, at least some used it for innocent purposes.[383] They too are now without their files. In many cases, users of one service are unaware that the first service in turn outsources to another service. Megaupload was a Software as a Service (or even Storage as a Service)

[381] Even though this was not always true. For example, it was important – and surprising to some – in the Yahoo! case that French traffic was actually directed through separate servers from North American traffic. Association Union des Etudiants Juifs de France v. Yahoo! Inc., *supra* note 245.

[382] This includes the case affecting Instapaper in Virginia and the Texas case that left at least one business unable to do business as the cloud service it relied on – and its data – were unavailable. Zetter, *supra* note 293; Kopytoff, *supra* note 293.

[383] As of the writing of this thesis none of the allegations against Megaupload and the alleged conspirators have been proven in any court. However, even accepting the allegations as fact, some percentage of Megaupload subscribers used the service for innocent purposes. See, *Indictment: United States of America v. Kim Dot Com, Megaupload, Inc., et. al.* (United States District Court for the Eastern District of Virginia, Alexandria Division, 2012) available online, <http://img.scoop.co.nz/media/pdfs/1201/78786408MegaIndictment.pdf>; Legitimate users face an uncertain fight to retrieve their non-infringing files. Gross, "Megaupload files might still be saved - CNN.com", *CNN*, online: <http://www.cnn.com/2012/01/30/tech/web/megaupload-data-deleted/index.html>; Martha Neil, "Those with Legitimate Content on Megaupload Site Raided by Feds Could Lose It in 'Data Genocide'", *ABA Journal* (30 January 2012), online: <http://www.abajournal.com/news/article/those_with_legitimate_content_on_megaupload_site_raided_by_feds_could_lose_/>.

product. However, it in turn outsourced its actual storage to two American companies.[384] Tracing the actual location of data and infrastructure in the cloud is not always an easy task.[385]

### 10.14 "The California Effect"

Much regulation of the Internet, and cloud applications upon it, has been decried as extra-territorial by users or governments not doing the regulating. For example, Yahoo! complained that France's ban on Nazi memorabilia would be unconstitutional in the United States because it would impose speech restrictions on a service originating in the United States. Likewise, the Australian decision in the *Gutnick* case came in for similar criticism – that it was an example of another country imposing a law that "puts at risk the ability of Americans to speak with each other and be protected by American law when they do so."[386] Likewise European privacy protections have been criticized as extraterritorial by some. For example, Microsoft famously changed its dot-NET passport application worldwide to comply with EU privacy laws and Google reluctantly added privacy information to comply with California law. In the arena of privacy protection, Europe exerts what Wu and Goldsmith call a "California effect." California, the most populous American state, typically imposes more stringent environmental protections than imposed federally. Manufacturers, especially of cars, find it cheaper to build one model meeting California's standards than to build multiple models for across the United States. Thus California has become the de-facto standard setter. What California has done for environmental protections, Europe has effectively done for privacy regulation.[387] States that

---

[384] According to the Megaupload indictment, as some members of the "Megaconspiracy" became concerned about U.S. legal action they questioned the wisdom of maintaining their data on U.S. servers. note 383 at 44 – 46.

Although it was first announced that all content would likely be deleted once Megaupload stopped paying its server hosting companies, the Electornic Frontier Foundation partnered with the hosting companies to launch project "MegaRetrieval". According to a statement, "EFF is troubled that so many lawful users of Megaupload.com had their property taken from them without warning and that the government has taken no steps to help them." "MegaRetrieval", (2012), online: <http://megaretrieval.com/>.

[385] As the Article 26 Working Party has noted; "Cloud computing makes it difficult to determine the location of personal data and of the equipment being used at any given time." Article 29 Working Party, *supra* note 325.

[386] Goldsmith & Wu, *supra* note 244 at 154 (quoting Floyd Abrams)..

[387] See Wu and Goldsmith, chapter 10.

are the first to occupy a given field can also have exercise a potent sort of first-mover advantage. Commentators have noted similarities between the processes by which Europe and the United States exerted outsize influence over privacy and securities regulation simply by being the first to make each area a priority.[388]

### 10.15 Overlapping effect is sometimes inevitable

Complaints decrying extraterritoriality are, however, usually one-sided. To allow American websites to operate with impunity would impose American law on the rest of the world. However, every other country has chosen to regulate speech more strictly than the United States. Likewise if cloud services (such as, for example, Facebook) originating in the United States did not follow EU privacy regulations the extra-territorial effect would be felt in Europe where EU citizens would be deprived of their privacy protections. Wu and Goldsmith call the "specter of multiple laws... exaggerated."[389] Most Internet users, they point out, will only ever be subject to the laws of their own country. On the other hand, multinationals that operate worldwide must comply with the laws of every country in which they operate. Johnson and Post's original ideas that activity on the web would be "simultaneously subject to the laws of all territorial sovereigns" meant it perhaps should be considered apart from traditional notions of jurisdiction. However, increasingly, borders are built into the Internet, Twitter's recent announcement being a prime example.

### 10.16 Outsize U.S. influence

The physical infrastructure of the Internet has left the United States with the practical ability influence events with very little apparent U.S. connection. The cases of Steve Marshall and Richard O'Dwyer provide example. Both were UK citizens who found out in surprising ways the role the U.S. government could play in their lives. Marshall lived in Spain and ran a number of

[388] Goldsmith & Wu, *supra* note 244; Newman, *supra* note 1.

[389] Goldsmith & Wu, *supra* note 244 at 159.

websites promoting travel to Cuba. He woke up one morning to find that 80 of his websites in various languages had been taken down at the request of U.S. authorities because they ultimately promoted travel to Cuba.[390] The shock must have been even greater for O'Dwyer. A college student, O'Dwyer ran a website that posted links to other sites where visitors could download infringing content. The illegality of the site would not have been certain in the United Kingdom. O'Dwyer is now facing extradition to the United States where he faces criminal charges that could land him in jail for years.

Neither webmaster hosted their content on servers in the United States. However, the domain name registrars responsible for the prestigious .com and .net domains are all within the United States. Thus, much traffic to such sites passes through the United States. The domain name registries tell your browser where to go when you type in a web address. Behind the scenes, websites have IP addresses composed of a string of numbers. Google owns several, including 209.85.225.103.[391] For every text-based web page request, a domain name server matches the website name to the IP address behind it. Every country has a "top level domain", for example, .uk for the United Kingdom or .ca for Canada.[392] These can stay within their respective countries. However, .com and .net are generally considered more desirable Internet real estate and are all based in the United States. In the view of the United States Treasury Department, this is enough. According to an official; "The jurisdiction we have over these sites right now really is the use of the domain name registry system in the United States. That's the key."[393] The official's comment highlights not only the confusing nature of determining jurisdiction in

---

[390] Adam Liptak, "A Wave of the Watch List, and Speech Disappears", *New York Times* (4 March 2008), online: <http://www.nytimes.com/2008/03/04/us/04bar.html>; Mirand Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law" (2009) 6:1 Scripted Journal of Law, Technology and Society 1, online: <http://www.hpl.hp.com/techreports/2009/HPL-2009-99.pdf>.

[391] Try it. Instead of typing Google.com, enter 209.85.225.103 in the navigation bar of a web browser. This is a Google North America IP address and might not work elsewhere.

[392] For example, www.mcgill.ca, which corresponds to 132.216.177.160. In the UK, www.bbc.co.uk for the BBC, which corresponds to 212.58.246.95

[393] Peter Walker, "US anti-piracy body targets foreign website owners for extradition", *The Guardian* (3 July 2011), online: <http://www.guardian.co.uk/technology/2011/jul/03/us-anti-piracy-extradition-prosecution>.

It will also be interesting to see whether a backlash against U.S. overreaching will impact commercial demand for .com, .net, or other sites handled by U.S. registrars.

the field of cloud computing and the Internet, but also the physical realities – location of server, power to enforce – that sometimes underlie it.

Among the many properties to be seized as per the January, 2012 indictment of the "Mega Conspiracy" behind the digital locker site Megaupload were several domain names, including the flagship "Megaupload.com". Upon application to the U.S. District Court for the Eastern District of Virginia, the sites were "seized" and turned over to the Department of Justice. Seizing a website is considerably different from seizing a physical object, although numerous allegedly ill-begotten objects were seized from the Megaupload conspirators. However, for the physical objects it was necessary for the American authorities to receive the help of New Zealand authorities; they had to actually go and grab the things in New Zealand. However, seizing a domain name instead involves ordering a domain name registry to direct Internet traffic otherwise directed for that site to a site of the government's choosing. This is because behind every web address, such as "www.megaupload.com" is an IP address defining the actual location of the site. Currently, for Megaupload, this is 107.21.243.42, which is a site owned by the U.S. Department of Justice announcing that the "domain name associated with the website Megaupload.com has been seized pursuant to an order issued by a U.S. District Court." A number of domain name services share responsibility for the allocation of domain names, like www.megaupload.com. These are in turn stored on the master "root" name server which then knows to match a name to a numeric IP address. Before the seizure by U.S. authorities, the root, which is duplicated throughout the world, would have known to match the name www.megaupload.com to a different IP address – the one where the actual website was hosted.

Internet addresses are grouped by "top level domains", such as the familiar ".com" or ".net". Each country also has its own generic top level domain, such as .ca for Canada, or .uk for the

United Kingdom, as well as numerous others that exist for special purposes.[394] Although the system is worldwide, the best real estate is governed from the United States, including all domain names ending in .com and .net. This means that American courts can quite easily exert influence over them by ordering a change in the numeric IP address to which visitors are directed. This happened en masse to over 150 sites deemed to be dedicated to piracy just before "Cyber Monday" in the lead-up to Christmas 2011. Now all the sites, including cheapjerseysite.org and uggbootsclearanceoutletstores.com redirect to 74.81.170.110, which has the same general look as the "seized" Megaupload site but slightly different wording.[395]

Some sites have attempted to limp along without the benefit of the domain name system. For example, the satirical site voteauction.com was meant to criticize the role of money in American politics. However, the Cook County, Illinois Elections Commissioners saw it as an illegal exercise in vote-selling. In the first case of the technique now favoured by antipiracy enforcement efforts, the Board of Elections Commissioners obtained a judgment from an Illinois state court ordering the domain name service Domain Bank to cancel the name www.voteauction.com. The site subsequently tried to exist outside of the domain name system by publicizing its numeric IP address. However, this proved far less catchy than the intended name.[396] Megaupload was reported to have continued for a few days after its shutdown by American authorities; if this is true then users with the numeric IP address would have been able to access the site for a few days after the domain name seizure. Some speculate that awareness of U.S. influence over popular top level domains including .com will spur the growth in popularity of alternatives such as national generic top level domain names, such as .ca or .uk.

---

[394] "List of Internet top-level domains - Wikipedia, the free encyclopedia",, online: <http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains#USA_top-level_domains>.

[395] US Immigration and Customs Enforcement, "Operation In Our Sites protects American online shoppers, cracks down on counterfeiters", (28 November 2011), online: *ICEgov* <http://www.ice.gov/news/releases/1111/111128washingtondc.htm> (with link to list of seized sites).

[396] Goldsmith & Wu, *supra* note 244.

The U.S. influence over the domain name registries is an artefact of the important U.S. role in funding in building the Internet. Like the domain name servers that provide a physical link to the United States, the preponderance of U.S. companies involved in cloud services provides additional links, either virtual or physical to the United States. The list of cloud providers is overwhelmingly American, from the giants such as Salesforce, Microsoft, Amazon, and Google, to smaller companies such as Dropbox, the list is overwhelmingly American. For the time being at least, using many cloud services will quite likely lead to further possible entanglements with U.S. [397]

[397] See, for example, the Filnet add playing on Patriot Act fears to promote "un cloud made in France." Filnet, *supra* note 219.

## 11. CONCLUSION

Europe has succeeded in making itself the global leader in privacy and consumer protections. Such protections do come with costs, as many cloud providers attest.[398] Within the EU, harmonisation is incomplete, leading to additional compliance costs for businesses, including potentially the need to comply with 27 separate legal regimes for some matters. Due to recognition of judgments within the EU, participation anywhere in the market can potentially mean exposure to liability anywhere in the market. Providers offering consumer services will certainly be wherever those services are marketed. In non-contractual matters, such as libel, jurisdiction in 27 nations is possible. In privacy matters – depending on the classification as a data controller or processor – jurisdiction will exist in at least one or more states. Some providers with no EU presence – like Twitter before its expansion – might be able to operate in some countries without realistic fear of enforcement of judgments against them; however, states do have the effective power to block or otherwise control sites within their borders. Cloud providers are also able to tailor their offerings for different markets, such as by limiting availability, or customizing terms of service or content for various countries.

The United States provides an environment that is overall more business friendly with the notable exception of the – probably exaggerated – fear of government surveillance. Exaggerated or not, such fear has caused some reluctance to deal with American providers. The possibility of becoming involved in American litigation discovery possibly has some impact as well on the attitudes of potential customers. Despite some difficulty and inefficiency presented by incompatibilities between U.S. and European regulations, such as the fact that the United States is not deemed to provide "adequate" data protection under the Data Protection Directive, data flows continue under regimes such as binding corporate rules, contracts, and the U.S. Safe Harbor program. Europe seems to be renewing its commitment to staying at the

---

[398] *Internet Privacy: The Impact and Burden of EU Regulation*, Paula Bruening, 15 September 2011 [*Internet Privacy: The Impact and Burden of EU Regulation*] (describing impact of EU regulations on U.S. providers) ; Google, *supra* note 252; Microsoft, *Microsoft's Response to the Commission's Public Consultation on Cloud Computing* (Brussels: Microsoft, 2011).

forefront of privacy protection with the unveiling of the new proposed updates to the Data Protection Directive. It seems safe to say that substantial differences will exist between U.S. and EU approaches for some time, meaning the technologist's desired "jurisdiction indifference" is nowhere in sight.

In early 2012, both Europe and the United States unveiled plans for new regulatory regimes in the field of privacy. Europe's proposed re-write of the Data Protection Directive sought to streamline compliance by harmonising the law throughout Europe.[399] However, it would also ratchet up privacy protections, including giving data subjects new rights, including the "right to be forgotten" to have data controllers purge the information they hold on specific people. In the United States, President Barrack Obama proposed a "Consumer Privacy Bill of Rights" that would nudge the United States closer to the European model of data protection but would, in characteristically American fashion, retain a role for industry self-regulation. Both the American and EU proposals are far from becoming law and could be subject to considerable change before they are passed, if ever become law. As the Obama proposal recognises, important differences exist between the American and European laws. These differences sometimes lead to difficulties that have commercial implications. Thus, a stated goal of the Obama plan is improving "interoperability" with other legal systems.[400]

Issues of privacy online and in the cloud have captured the attention of the public, press, and government to an extraordinary degree in recent days, which underscores the growing awareness that such issues will be increasingly important in the years ahead. It is in this context that we should consider the legal issues surrounding cloud computing. Cloud computing promises great advantages to business and consumers, yet is premised on the free flow of information across the globe. From time to time, law presents a major impediment to

[399] European Commission, *supra* note 91 (As a regulation instead of a directive, the new proposal would have direct effect across the Europe.

[400] Obama, *supra* note 147("The United States will engage with our international partners to create greater interoperability among our respective privacy frameworks").

such information flows. There are strong factors that favour allowing law to get out of the way in the name of efficiency. However, states can and do come to differing conclusions about the best balances between competing values such as free speech, privacy, or consumer protections. Although laws lack of "interoperability" can slow global commerce dependent on information flows, it is also a by-product of decisions states have made regarding important issues about protecting individuals in the field of privacy and consumer rights.

The United States has exported the world's leading cloud computing technologies and companies. Europe, by contrast has stood firm in its commitment to consumer and privacy protections, which it has also managed to export to much of the world. The growing concerns about privacy in the United States are at least in part influenced by the example Europe has set in terms of protecting personal privacy. Of course, the concern for privacy and support for privacy regulations could arise simultaneously in different places; the United States does not need to follow Europe's experience to note the "creep factor" possible from abuse of personal data or that discrimination based on such data risks undermining social cohesion.[401] However, European experience has provided a model that will at least be influential for any future American privacy regulation. This is clear from the Obama document's promise to "engage with our international partners to create greater interoperability among our respective privacy frameworks."[402] This will not necessarily represent convergence as the EU seems likewise set to tighten privacy regulations in the direction of greater protection for consumers. The United States may soon tread territory first explored by the EU, although in an American style. This is evidenced by the Obama administration's stated desire to pursue, "Enforceable codes of conduct, developed through multistakeholder processes."[403] While efforts such as that of the Obama administration seek to increase "interoperability", cloud providers have also shown a

[401] Turow, *supra* note 69.

[402] Obama, *supra* note 202.

[403] *Ibid*.

remarkable ability to adapt to the real-world conditions of a fragmented global market and conflicting legal demands.

### 11.1 Recent events – pushing the limits

In February, 2012 the Internet giant Google announced that it would begin sharing information across its services. Thus information gleaned from one Google property, for example, YouTube, would then be shared with others such as Google's flagship search engine or Gmail service. Gmail has always offered free email subsidized by user information gleaned from the content of emails. Previously information was compartmentalized among services. Under the new plan, for example, frequent searches for rock music videos on YouTube might lead to a crop of ads for albums or concerts alongside emails in users' Gmail accounts. Under the new rules that went into effect March 1, 2012, nearly all of Google's 60 or so services now share information.[404] The changes will also purportedly help Google offer improved user experiences, for example by better customizing search results. Google says part of the goal is to "create one beautifully simple and intuitive experience across Google."[405]

However, on both sides of the Atlantic outrage ensued at the fact that Google was changing the terms of its bargain with its users. In the United States, Politicians expressed alarm at the new policy changes and the Electronic Privacy Information Center (EPIC) sued the U.S. Federal Trade Commission (FTC) to try to force the agency to stop the planned change.[406] Although thirty U.S.

---

[404] Users can see some of the information Google has about them at Google's "Dashboard": Google Inc, "Google Accounts", (2012), online: *Google* <https://www.Google.com/dashboard>.

Wikipedia offers a list of Google products: http://en.wikipedia.org/wiki/Google_products#Mobile_applications

[405] *See*, Google explanation of the new policy: Wikipedia contributors, *List of Google products* (Wikimedia Foundation, Inc., 2012).

[406] *Electronic Privacy Information Center v. The Federal Trade Commission*, (available on http://epic.org/privacy/ftc/google/EPIC-Complaint-Final.pdf) (complaint by EPIC).

state attorneys general signed a letter saying they found the change "troubling."[407] Although the EPIC lawsuit failed, the issue decided was only that EPIC could not force the FTC to commence an action or investigation.[408] The FTC may still be investigating the Google privacy changes at its own pace. In Europe, regulators, led by France's Commission nationale de l'informatique et des libertés (CNIL) issued a statement saying in their belief the new Google policies would violate European privacy law under the Data Protection Directive, 95/46/EC.[409] The CNIL's opinion is not the final say on the legality of Google's plans, but certainly should have been persuasive and an indication of the likelihood possible legal trouble ahead. Nevertheless, Google went ahead and instituted the new policies on March 1, 2012. These developments plucked from recent headlines illustrate two themes. On the one hand, concern for privacy protections – typically associated more with Europe than the United States – may be growing in the United States. Despite this, the more robust response from European regulators, lead by France, illustrates the continuing differences between the two regimes. Google's response illustrates the manner in which cloud providers can be counted on to test the limits of what they can do under the law.

### 11.2 Jurisdiction in the Right Way

The cloud has much to offer in both increased efficiency and brand new services that simply were not available before. However, it also exacerbates serious problems of differing regulatory regimes and jurisdictional conflict that have gathered pace since the advent of the Internet. In the extreme, conflicts between countries threaten the existence of the cloud itself.

---

[407] National Association of Attorneys General, *National Association of Attorneys General letter of Feb. 22, 2012 to Larry Page of Google, Inc.* (National Association of Attorneys General, 2012) online, <http://www.naag.org/assets/files/pdf/signons/20120222.Google%20Privacy%20Policy%20Final.pdf>.

[408] *Electronic Privacy Information Center v. Federal Trade Commission*, 2012 Civil Action No. 12-0206 (ABJ) (available on http://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf) (memorandum opinion).

[409] CNIL, *supra* note 243 online, <http://www.cnil.fr/english/news-and-events/news/article/googles-new-privacy-policy-raises-deep-concerns-about-data-protection-and-the-respect-of-the-euro/>.

Take the example presented by the use of cloud applications in some Canadian contexts; local options often simply do not exist. A service like Gmail or Google apps for education might make sense to build for a worldwide market, but not for a single-country market. If a local option was built, it might well be a lesser product, more expensive, or both. It especially does not make sense to limit the locations of cloud infrastructure. Great care is taken to find the most efficient locations for infrastructure such as data centers and legal restrictions can distort these choices leading to duplication of efforts or the development of infrastructure in sub-optimal locales. Given the growing energy consumption of cloud computing infrastructure and the impact choice of location can have on energy use, it makes sense to leave all options on the table.

On the other hand, very important choices about cultural values inform the law affecting the cloud, chiefly in terms of privacy and consumer protection. One commentator has noted the difference in attempting to negotiate privacy agreements as opposed to other areas such as copyright; "[P]rivacy questions seem to touch closer to the nation's psyche, and even culturally similar nations differ profoundly over what they consider 'adequate' in the regulation of privacy."[410] With differences so pronounced between the United States and Europe, the two biggest cloud computing markets, it seems both implausible and undesirable to push for the type of convergence that might eliminate the existing problems.

In this spirit, a few legal and technical possibilities do add hope. First and foremost, jurisdictional rules should focus on who the actual users of a service, especially targeted users, are. An aspect of this was seen in the *Young v. New Haven Advocate* decision noted above when the U.S. 4th Circuit ruled that jurisdiction was not proper because the newspaper had not targeted West Virginia.[411] Similarly admirable restraint was shown in the Scottish *Bonnier*

[410] Tim Wu, "The International Privacy Regime" in Anupam Chander, Lauren Gelman & Margaret Jane Radin, eds, *Securing Privacy in the Internet Age* (Stanford: Stanford University Press, 2008) at 95.

[411] Young v. New Haven Advocate, *supra* note 315.

*Media* case.[412] In cases such as *Guttnick*, where a specific jurisdiction has been targeted, especially when a publisher has the option to avoid a certain market, jurisdiction should still be proper.[413] In other areas as well, targeting should be the touchstone. For example, if a cloud service not directed at Europeans inadvertently attracts European users, this should not necessarily subject it to European privacy laws in the handling of data. The specifics of this may change over time so as to avoid sham claims not to target a jurisdiction. For example, the *iCraveTV* approach of asking for a telephone area code to prove residence was probably a sham in any era. However, while IP address verification is currently fairly accepted to verify residence, for example as Pandora and Hulu do to avoid broadcasting in Canada, if more consumers become aware of ways to circumvent this method, it may be necessary to revise standards upward. Governments can also help by adopting "good neighbour", policies as Australia the United Kingdom have done in the field of gambling. Both allow Internet gambling operations but make it a local offense to target countries where gambling is illegal.[414] Countries should also assess the impact of laws such as the USA Patriot Act or Sweden's law permitting the inspection of data crossing its frontiers which make the home country inappropriate to many as a cloud host location. There is even some precedent for another type of restraint in idea of offshore data areas. China has announced plans to build a special cloud computing zone near Chongqing where foreign companies will have access to the full Internet without the typical Chinese restrictions.[415] For many purposes, Hong Kong already serves a similar role for China, as it is already a popular location for providers such as Google who find business in mainland China difficult. Similarly, Dubai touts its Dubai International Finance Centre, where EU-compliant data protection law has been implemented.[416] In an effort to attract processing

[412] Bonnier Media v. Kestrel Trading Corp. *supra* note 333

[413] Dow Jones and Company Inc v Gutnick, *supra* note 331.

[414] United Kingdom: Gambling Act. s.44, Australia: Section 15A of the Interactive Gambling Act 2001 (Cth).

[415] Asia Cloud Forum Staff, "China builds 10 sq km cloud computing special zone in Chongqing | Asia Cloud Forum", (2 March 2011), online: <http://www.asiacloudforum.com/content/china-builds-10-sq-km-cloud-computing-special-zone-chongqing>.

[416] "DIFC Data Protection Law", online: <http://dp.difc.ae/>.

business, France has exempted companies with no operations in France from many data protection requirements if they use French cloud providers.[417] Perhaps the United States could also consider pragmatic measures to reassure would-be users of U.S. services.

Technology could also play a role in alleviating some issues. As encryption techniques become better it may be possible to encrypt more data in the cloud making users less worried about where it is eventually stored. Encrypted information is already considered outside EU privacy regulations in many instances.[418] However, limitations exist on what can be done with data while it is encrypted. Currently, while storage or transit of encrypted data is usually possible, performing any computing operations on it becomes inefficient. Also, without some tolerance from government, companies that are too good at encryption will face problems. This has essentially been Blackberry's problem that got the company banned from a number of countries.[419]

The world will be best served if the problems of jurisdiction and conflicting laws can be addressed so as to permit the benefits of a truly global cloud. However, this should not come at the expense of national values. If solutions cannot be implemented through legal or technical means, perhaps the next-best solution would be a continued uneasy, yet still mostly functional coexistence of very different regimes.

---

[417] CNIL, *Deliberation no. 2011-023* (CNIL, 2011).

[418] Hon, Millard & Walden, *supra* note 5.

[419] Zack Whittaker, "BlackBerry encryption 'too secure': National security vs. consumer privacy | ZDNet", (29 July 2010), online: <http://www.zdnet.com/blog/igeneration/blackberry-encryption-too-secure-national-security-vs-consumer-privacy/5732>.

Internet Privacy: The Impact and Burden of EU Regulation, Paula Bruening, 15 September 2011 [Internet Privacy: The Impact and Burden of EU Regulation]

ECPA Reform and the Revolution in Cloud Computing, Mike Hintze, 23 September 2010 [ECPA Reform and the Revolution in Cloud Computing]

Protecting Children from Predators Act, Vic Toews, February 2012 [C-30]

European Convention on Human Rights 8.1, 1950 [ECHR 8.1]

Right to Financial Privacy Act., 1978, 12 USC 3401 et seq [RFPA]

Law No. 80-538 of July 16, 1980, 16 July 1980 [Law No. 80-538 of July 16, 1980]

Electronic Communications Privacy Act, 1986, 27 USC 2701 et seq [ECPA]

Electronic Communications Privacy Act, 1986, 18 USC 2701 et seq [Electronic Communications Privacy Act]

Data Protection Directive, 1995 [95/46/EC]

47 U.S.C. 230, 1996 [Communications Decency Act]

Digital Millenium Copyright Act, 1998, 17 USC 512 [D.M.C.A. § 512]

Financial Services Modernization Act of 1999, 1999, 15 USC § 6801 - 6809 [Gramm Leach Bliley Act]

45 C.F.R. 160.202, 2000, Code of Federal Regulations (US) [45 C.F.R. 160.202]

2000/31/EC, 2000 [Directive on Electronic Commerce]

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, 2000, 44/2001 [EC 44/2000]

USA Patriot Act, 1 February 2002 [Patriot Act]

Online Privacy Protection Act of 2003, 2003, Cal Bus & Prof Code 22575-22579 [Online Privacy Protection Act of 2003]

California Security Breach Notification Law, SB 1386, 2003, California Civil Code 179829, 179882, 179884 [California Security Breach Notification Law, SB 1386]

Massachusetts General Law Chapter 93H, 2009 [Massachusetts General Law Chapter 93H]

Privacy Act, 5 USC section 552A [Privacy Act of 1974]

Perrin, R v [2002] EWCA Crim 747 (22nd March, 2002), 2002 (available on http://www.bailii.org/ew/cases/EWCA/Crim/2002/747.html)

CTB v News Group Newspapers Ltd & Anor [2011] EWHC 1232 (QB), 2011 (available on http://www.bailii.org/ew/cases/EWHC/QB/2011/1232.html)

Association Union des Etudiants Juifs de France v. Yahoo! Inc. (2000), 6 2000 ILR Nov. 20, 2000 434

Pennoyer v. Neff (1878), 95 1878 US 714

Olmstead v. United States (1928), 277 1928 US 438

International Shoe Co. v. Washington (1945), 326 1945 US 310

Shibley v. Time, Inc (1975), 45 1975 Ohio App 2d 69

United States v. Miller (1976), 425 1976 US 435

Whalen v. Roe (1977), 429 1977 US 589

Helicopteros Nacionales de Colombia, SA v. Hall (1984), 466 1984 US 408

Calder v. Jones (1984), 465 1984 US 783

Societe Nationale Industrielle Aerospatiale v. District Ct. for the S. Dist. of Iowa (1987), 482 1987 US 522

Asahi Metal Industry Co. v. Superior Court of Cal., Solano Cty. (1987), 480 1987 US 102

Carnival Cruise Lines, Inc. v. Shute (1991), 499 1991 US 585

Dwyer v. American Exp. Co. (1995), 652 1995 NE 2d 1351

ProCD, Inc. v. Zeidenberg (1996), 86 1996 F 3d 1447

Zippo Mfg. Co. v. Zippo Dot Com, Inc. (1997), 952 1997 F Supp 1119

Condon v. Reno (1998), 155 1998 F 3d 453

Millennium Enterprises v. Millennium Music, LP (1999), 33 1999 F Supp 2d 907

People v. World Gaming Corp (1999), 185 1999 Misc 2d 852

Reno v. Condon (2000), 528 2000 US 141

Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme (2001), 169 2001 FSupp2d 1181

Toben (2001), 8 2001 Neu Juristische Wochenschrift 624

Muick v. Glenayre Electronics (2002), 280 2002 F 3d 741

Young v. New Haven Advocate (2002), 315 2002 F 3d 256

Gorman v. Ameritrade Holding Corp. (2002), 293 2002 F 3d 506

Dow Jones and Company Inc v Gutnick, 2002 56 (available on http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html)

Doe v. Ashcroft (2004), 334 2004 F Supp 2d 471

American Bar Ass'n v. FTC (2005), 430 2005 F 3d 457

Yahoo! Inc. v. La Ligue Contre Le Racisme (2006), 433 2006 F 3d 1199

Bragg v. Linden Research, Inc. (2007), 487 2007 F Supp 2d 593

Doe v. Friendfinder Network, Inc. (2008), 540 2008 F Supp 2d 288

Forward Foods Llc v. Next Proteins, Inc. (2008), 2008 2008 NY Slip Op 52058

PROCUREUR-GENERAAL BIJ HET HOF VAN BEROEP TE GENT, eiser, tegen YAHOO! Inc., 2010 Nr P101347N (available on http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20110118-1)

Sorrell v. IMS Health Inc. (2011), 131 2011 S Ct 2653 (available on http://scholar.google.ca/scholar_case?case=838098438403992670&hl=en&as_sdt=2&as_vis=1&oi=scholarr)

In re Application of the United States of America for an order pursuant to 18 U.S.C. 2703(d) (memorandum opinion), 2011 1:11-DM-3 (available on http://www.aclu.org/files/assets/twitter_mem_op_11.10.2011.pdf)

US v. Jones (2012), 132 2012 S Ct 945

Electronic Privacy Information Center v. Federal Trade Commission, 2012 Civil Action No. 12-0206 (ABJ) (available on http://epic.org/privacy/ftc/google/EPICvFTC-CtMemo.pdf)

Flagg v. City of Detroit, 252 FRD 346

Electronic Privacy Information Center v. The Federal Trade Commission, (available on http://epic.org/privacy/ftc/google/EPIC-Complaint-Final.pdf)

Berners-Lee, Tim & Mark Fischetti. Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor (Paw Prints, 2008)

Carr, Nicholas G. Does IT matter?: information technology and the corrosion of competitive advantage (Harvard Business Press, 2004)

Carr, Nicholas G. The Big Switch: Rewiring the World, from Edison to Google (W. W. Norton and Company, 2011)

Deibert, Ronald. Access Denied: The Practice and Policy of Global Internet Filtering (MIT Press, 2008)

Goldsmith, Jack & Tim Wu. Who Controls the Internet? Illusions of a Borderless World (Oxford: Oxford University Press, 2006)

Hanloser, Stefan & Catrien Noorda, eds. E-Discovery and Data Privacy: A Practical Guide (Alpen aan den Rijn, NL: Wolters Kluwer, 2010)

Kohl, Uta. Jurisdiction and the Internet: Regulatory Competence over Online Activity (Cambridge: Cambridge University Press, 2007)

Kuner, Christopher. European Data Protection Law: Corporate Compliance and Regulation (Oxford University Press, 2007)

Mayer-Schönberger, Viktor. Delete: the virtue of forgetting in the digital age (Princeton University Press, 2009)

Newman, Abraham L. Protectors of Privacy: Regulating Personal Data in the Global Economy (Ithaca, NY: Cornell University Press, 2008)

Palfrey, John G, OpenNet Initiative & Rafal Rohozinski. Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (MIT Press, 2010)

Turow, Joseph. The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth (Yale University Press, 2012)

Babcock, Charles. "User Alliance Wants Cloud Interoperability", InformationWeek (8 June 2011), online: <http://www.informationweek.com/news/cloud-computing/infrastructure/230400015>

Barnett, Katy. "Twitter Undoes UK Super Injunctions «", The Fortnightly Review of IP & Media Law (2 June 2011), online: <http://fortnightlyreview.info/2011/06/02/twitter-undoes-uk-super-injunctions/>

boyd, danah & Eszter Hargittai. "Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act'" (2011) 16:11 First Monday, online: <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3850/3075>

Catan, Thomas & Amir Efrati. "Feds to Launch Probe of Google", Wall Street Journal (24 June 2011), online: <http://online.wsj.com/article/SB10001424052702303339904576403603764717680.html>

Cavajal, Doreen. "Vigilance: Where to set limits?", New York Times (21 April 2004), online: <http://www.nytimes.com/2004/04/21/business/worldbusiness/21iht-workcol21_ed3_.html>

Clifford, Stephanie. "Demand at Target For Fashion Line Crashes Web Site", The New York Times (13 September 2011), online: <http://www.nytimes.com/2011/09/14/business/demand-at-target-for-fashion-line-crashes-web-site.html>

Crossman, Penny. "Fieldpoint Private Bank Turns to Cloud Computing for CRM and Beyond", InformationWeek (13 July 2010), online: <http://www.informationweek.com/news/225702942>

Danadio, Rachel. "Larger threet is seen in Google case", New York Times (24 February 2010), online: <http://www.nytimes.com/2010/02/25/technology/companies/25google.html>

Dumbill, Ed. "Big data in the cloud", O'Reilly Radar (22 February 2012), online: <http://radar.oreilly.com/2012/02/big-data-in-the-cloud-microsoft-amazon-google.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+oreilly%2Fradar%2Fatom+%28O%27Reilly+Radar%29>

Easterbrook, Frank H. "Cyberspace and the Law of the Horse" (1996):1996 University of Chicago Legal Forum 207, online: <http://www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf>

Editors. “Twitter to block super injunction tweets in Britain”, TNT Magazine (31 January 2012), online: <http://www.tntmagazine.com/news/games/twitter-to-block-super-injunction-tweets-in-britain>

Essers, Loek. “European Data Concerns Cloud Outlook for US Vendors”, PCWorld (16 September 2011), online: <http://www.pcworld.com/businesscenter/article/240161/european_data_concerns_cloud_outlook_for_us_vendors.html>

Essers, Loek. “Dutch government set to block US cloud IT providers”, CIO (20 September 2011), online: <http://www.cio.co.uk/news/3304573/dutch-government-set-to-block-us-cloud-it-providers/>

Fay, Joe. “MobileMe drove Steve Jobs to foul-mouthed fury”, The Register (9 May 2011), online: <http://www.theregister.co.uk/2011/05/09/jobs_swear/>

Feinstein, Jeremy D. “Tying Up the Cloud: A Study in Antitrust Issues in Cloud Computing” in Transcending the Cloud: A Legal Guide to the Risks and Rewards of Cloud Computing (Reed Smith, 2010)

Fernandes, Joel. “Creating a Google Plus Account Now Requires You to Enter Your Birthday”, Techie Buzz (27 August 2011), online: <http://techie-buzz.com/social-networking/google-age-restrictions.html>

Fitzgerald, Michael. “How Visa Protects Your Data”, Fast Company, online: <http://www.fastcompany.com/magazine/160/visa-secret-security-center>

Fortado, Lindsay & James Lumley. “Twitter Inc., Unknown Posters Sued by Athlete Known as ‘CTB’ at U.K. Court”, Bloomberg (20 May 2011), online: <http://www.bloomberg.com/news/2011-05-20/twitter-inc-unknown-posters-sued-by-athlete-known-as-ctb-at-u-k-court.html>

Gamvros, Anna. “Hong Kong and China Taking Different Routes to the Cloud”, BNA International (March 2011), online: <http://www.bnai.com/HongKongChinaCloud/default.aspx>

Geist, Michael A. “Is There a There There? Towards Greater Certainty for Internet Jurisdiction” SSRN eLibrary, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=266932>

Gere, Duncan. “Spending a week with Chrome OS - Chrome OS review & test (Wired UK)”, Wired UK, online: <http://www.wired.co.uk/news/archive/2011-04/4/a-week-with-chromeos>

German Law Journal. “Federal Court of Justice (BGH) Convicts Foreigner for Internet Posted Incitement to Racial Hatred” (2001) 2 German Law Journal, online: <http://www.germanlawjournal.com/article.php?id=67>

Goldfarb, Avi & Catherine Tucker. “Privacy Regulation and Online Advertising” (2010) SSRN eLibrary, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1600259>

Goldsmith, Jack L & University of Chicago Law School. “Against cyberanarchy” (1998) 65 U Chi L Rev 1199, online: <http://groups.csail.mit.edu/mac/classes/6.805/articles/goldsmith-against-cyberanarchy.html>

Gottridge, Marc & Thomas Rouheete. “France puts some muscle behind its blocking statute”, New York Law Journal (29 April 2008), online: <http://www.hoganlovells.com/files/Publication/ed20ea51-6c49-4798-bd10-54c6f58f51b5/Presentation/PublicationAttachment/194fc242-489a-4db5-8ba1-a82bf053cdcd/France_Puts_Some_Muscle_Behind_Its_Blocking_Statute_29_04_08.pdf>

Gross. “Megaupload files might still be saved - CNN.com”, CNN, online: <http://www.cnn.com/2012/01/30/tech/web/megaupload-data-deleted/index.html>

Hanson, Craig. “Next World Capital”, New World Capital (2012), online: <http://www.nextworldcap.com/newsletter/article.php?id=1>

Hardy, Quentin. “The Big Business of ‘Big Data’ - NYTimes.com”, New York Times (24 October 2011), online: <http://bits.blogs.nytimes.com/2011/10/24/big-data/>

Harris, Edward C. “Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show that Europe Does Not Have the Answers” (2007) 22 Am U Int’l L Rev 745, online: <http://works.bepress.com/edward_harris/2/>

Helft, Miguel. “Facebook Chooses North Carolina for New Data Center”, New York Times (11 November 2010), online: <http://bits.blogs.nytimes.com/2010/11/11/facebook-chooses-north-carolina-for-new-data-center/>

Hon, W Kuan, Julia Hornle & Christopher Millard. “Data Protection Jurisdiction and Cloud Computing - When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3” (2012), online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1924240>

Hon, W Kuan, Christopher Millard & Ian Walden. “The Problem of ‘Personal Data’ in Cloud Computing - What Information Is Regulated? The Cloud of Unknowing, Part 1” (2011) SSRN eLibrary, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577>

Horn, Leslie. “Facebook Picks Sweden For First Data Center Outside U.S.”, PC Mag (27 October 2011), online: <http://www.pcmag.com/article2/0,2817,2395378,00.asp>

Horowitz, Steven J. “Defusing a Google Bomb” (2007) 117 Yale Law Journal Pocket Part 1, online: <http://yalelawjournal.org/the-yale-law-journal-pocket-part/intellectual-property/defusing-a-Google-bomb/>

Johnson, David R & David G Post. “Law and Borders: The Rise of Law in Cyberspace” (1996) 48 Stan L Rev 1367, online: <http://cyber.law.harvard.edu/is02/readings/johnson-post.html>

Kavur, Jenni. “Don’t use the Patriot Act as an excuse”, ComputerWorld Canada (5 July 2010), online: <http://www.itworldcanada.com/news/dont-use-the-patriot-act-as-an-excuse/141033>

Kerr, Orin. “The Case for the Third Party Doctrine” (2009) 107 Mich L Rev 561, online: <http://mlr.stereodevelopment.com/assets/pdfs/107/4/kerr.pdf>

Kopytoff, Verne G. “F.B.I. Seizes Web Servers, Knocking Sites Offline”, Bits Blog (21 June 2011), online: <http://bits.blogs.nytimes.com/2011/06/21/f-b-i-seizes-web-servers-knocking-sites-offline/>

Kuner, Christopher. “Data Protection Law and International Jurisdiction on the Internet (Part 1)” (2010) 18:2 IJLIT 176

Leach, Ann. “Facebook’s Swedish data centre will be subject to Snoop Law • The Register”, The Register (31 October 2011), online: <http://www.theregister.co.uk/2011/10/31/facebook_swedish_data_centre_privacy_law/>

Lessig, Lawrence. “The Law of the Horse: What Cyberlaw Might Teach” (1999) 113 Harv L Rev 501, online: <http://www.lessig.org/content/articles/works/finalhls.pdf>

Liptak, Adam. “A Wave of the Watch List, and Speech Disappears”, New York Times (4 March 2008), online: <http://www.nytimes.com/2008/03/04/us/04bar.html>

MacDonald, Allison. “Youtubing Down the Stream of Commerce: Eliminating the Express Aiming Requirement for Personal Jurisdiction in User-Generated Internet Content Cases” (2009) 19 Alb LJ Sci & Tech 519, online: <http://www.albanylawjournal.org/articles/MacDonald_Format_YS.pdf>

Matwyshyn, Andrea M. “Introduction” in Harboring Data: Information Security, Law, and the Corporation (Stanford: Stanford University Press, 2009)

Miller, Rich. “Microsoft Picks Virginia for Major Data Center » Data Center Knowledge”, Data Center Knowledge, online: <http://www.datacenterknowledge.com/archives/2010/08/27/microsoft-picks-virginia-for-major-data-center/>

Moshell, Ryan. “And then there was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection” (2005) 37 Texas Tech L Rev 357

Mowbray, Mirand. “The Fog over the Grimpen Mire: Cloud Computing and the Law” (2009) 6:1 Scripted Journal of Law, Technology and Society 1, online: <http://www.hpl.hp.com/techreports/2009/HPL-2009-99.pdf>

Neil, Martha. “Those with Legitimate Content on Megaupload Site Raided by Feds Could Lose It in ‘Data Genocide’”, ABA Journal (30 January 2012), online: <http://www.abajournal.com/news/article/those_with_legitimate_content_on_megaupload_site_raided_by_feds_could_lose_/>

Nimmer, Raymond T. “Contracts, Markets, and Data Control” in Securing Privacy in the Internet Age (Stanford: Stanford University Press, 2008)

Noorda, Catrien & Stefan Hanloser. “EU Data Privacy Regulations” in E-Discovery and Data Privacy: A Practical Guide (Frederick, MD: Wolters Kluwer, 2011)

O’Brien, Kevin J. “Europe Turns to the Cloud”, The New York Times (24 July 2011), online: <http://www.nytimes.com/2011/07/25/technology/europe-turns-to-the-cloud.html>

Palmer, Maija. “Where the Internet Lives”, Financial Times (17 February 2009), online: <http://www.ft.com/cms/s/0/878ac3ba-d31b-11de-af63-00144feabdc0.html>

Peek, Marcy E. “Beyond Contract: Utilizing Restitution to Reach Shadow Offenders and Safeguard Information Privacy” in Anupam Chander, Lauren Gelman & Margaret Jane Radin, eds, Securing Privacy in the Internet Age (Stanford: Stanford University Press, 2008)

Retzer, Karin & Michael Miller. “Mind the Gap: U.S. Discovery Demands versus EU Data Protection”, BNA Privacy and Security Law Report (13 June 2011), online: <http://www.mofo.com/files/Uploads/Images/110601-US-Discovery-Demands-versus-EU-Data-Protection.pdf>

Satow, Julie. “In Former New York Telephone Tower, Sabey Corp. Plans Data Centers”, The New York Times (14 February 2012), online: <http://www.nytimes.com/2012/02/15/realestate/commercial/in-former-new-york-telephone-tower-sabey-corp-plans-data-centers.html>

Seigler, MG. “The Web Collapses Under the Weight of Michael Jackson’s Death”, Tech (25 June 2009), online: <http://techcrunch.com/2009/06/25/the-web-collapses-under-the-weight-of-michael-jacksons-death/>

Sengupta, Somini. “When Twitter Blocks Tweets, It’s #Outrage”, The New York Times (27 January 2012), online: <http://www.nytimes.com/2012/01/28/technology/when-twitter-blocks-tweets-its-outrage.html>

Singel, Ryan. “Twitter’s Response to WikiLeaks Subpoena Should Be the Industry Standard”, Wiredcom (10 January 2011), online: <http://www.wired.com/threatlevel/2011/01/twitter/>

Singel, Ryan. “Dropbox Lied to Users About Data Security, Complaint to FTC Alleges”, Wired (13 May 2011), online: <http://www.wired.com/threatlevel/2011/05/dropbox-ftc/#more-26298>

Slaughter, Dana & Wang Zhenlin. “Information Security of Children’s Data: From ‘Ego’ to ‘Social Comparison’ - Cultural Transmission and Child Data Protection Policies and Laws in a Digital Age”

in Harboring Data: Information Security, Law, and the Corporation (Stanford: Stanford University Press, 2009)

Smith, Catherine. "7,500 Online Shoppers Accidentally Sold Their Souls To Gamestation", Huffington Post (17 April 2010), online: <http://www.huffingtonpost.com/2010/04/17/gamestation-grabs-souls-o_n_541549.html>

Soghoian, Christopher. "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era" (2009) 8 J on Telecomm and High Tech L 359, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1421553&http://www.google.com/url?sa=t&source=web&cd=3&sqi=2&ved=0CCwQFjAC&url=http%3A%2F%2Fpapers.ssrn.com%2Fsol3%2FDelivery.cfm%2FSSRN_ID1656471_code636196.pdf%3Fabstractid%3D1421553%26mirid%3D1&rct=j&q=soghoian%20cloud%20market%20failure&ei=BUXuTfzHD8zAgQf3o7yUDw&usg=AFQjCNFwsUqzpHWL8S3OWBHisYE80gDS8w&sig2=IiejGHaeb_7j9uMISbQ2IQ>

Todd, Phillip. "Switch to Google e-mail saves resources, raises privacy concerns", University Affairs (10 March 2008), online: <http://www.universityaffairs.ca/switch-to-Google-email-saves-resources-raises-privacy-concerns.aspx>

Trappler, Timothy. "If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues", Educase Quarterly (2010), online: <http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfItsintheCloudGetItonPaperClo/206532>

Troianovski, Anton. "Storage Wars: Web Growth Sparks Data-Center Boom", Wall Street Journal (7 July 2011), online: <http://online.wsj.com/article/SB10001424052702303763404576417531646400002.html>

Walden, Ian & Laise Da Correggio Luciano. "Ensuring Competition in the Clouds: The Role of Competition Law?" (2011) SSRN eLibrary, online: <http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1840547>

Walker, Peter. "US anti-piracy body targets foreign website owners for extradition", The Guardian (3 July 2011), online: <http://www.guardian.co.uk/technology/2011/jul/03/us-anti-piracy-extradition-prosecution>

White, Aoife. "Can Ireland's Regulators Stand Up for Internet Privacy?", BusinessWeek: Magazine (9 February 2012), online: <http://www.businessweek.com/magazine/can-irelands-regulators-stand-up-for-internet-privacy-02092012.html>

Whitman, James Q. "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113 Yale L J 1151, online: <http://www.yalelawjournal.org/the-yale-law-journal/content-pages/the-two-western-cultures-of-privacy:-dignity-versus-liberty/>

Whittaker, Zack. "Why is Canada reluctant to adopt cloud computing?", ZDNet (15 June 2010), online: <http://www.zdnet.com/blog/igeneration/why-is-canada-reluctant-to-adopt-cloud-computing/5314>

Whittaker, Zack. "BlackBerry encryption 'too secure': National security vs. consumer privacy | ZDNet", (29 July 2010), online: <http://www.zdnet.com/blog/igeneration/blackberry-encryption-too-secure-national-security-vs-consumer-privacy/5732>

Whittaker, Zack. "Microsoft admits Patriot Act can access EU-based cloud data", ZDNet (28 June 2011), online: <http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225>

Wood, Lamont. "Cloud computing and compliance: Be careful up there", Computerworld (30 January 2009), online:

<http://www.computerworld.com/s/article/9126934/Cloud_computing_and_compliance_Be_careful_up_there_>

Wu, Tim. "The International Privacy Regime" in Anupam Chander, Lauren Gelman & Margaret Jane Radin, eds, Securing Privacy in the Internet Age (Stanford: Stanford University Press, 2008)

"SA pigeon 'faster than broadband'", BBC Online (10 September 2009), online: <http://news.bbc.co.uk/2/hi/8248056.stm>

"Google convictions reveal two flaws in EU law, not just Italian law", Pinsent Mansons Out-Law (3 March 2010), online: <http://www.out-law.com/page-10805>

"Amazon cloud uses FedEx instead of the Internet to ship data", Network World (10 June 2010), online: <http://www.networkworld.com/news/2010/061010-amazon-cloud-fedex.html>

"Apple's North Carolina iCloud Data Center Finally Appears on Google Maps", (1 June 2011), online: <http://www.huffingtonpost.com/2011/06/01/apple-data-center_n_869596.html>

"Twitter Ignored Request To Keep Subpoena Under Wraps [UPDATED]", ReadWriteWeb (27 December 2011), online: <http://www.readwriteweb.com/archives/twitter_ignored_request_to_keep_subpoena_under_wraps.php>

"Greenpeace scorecard documents greener enterprise offerings", Computerworld (8 February 2012), online: <http://www.computerworld.com/s/article/9224063/Greenpeace_scorecard_documents_greener_enterprise_offerings>

"Google says its new privacy policy complies with FTC settlement", latimescom (10 February 2012), online: <http://www.latimes.com/business/technology/la-fi-tn-google-privacy-ftc-20120210,0,5736133.story>

"Apple's invisible data center finally appears on Google Earth", Technolog, online: <http://www.technolog.msnbc.msn.com/technology/technolog/apples-invisible-data-center-finally-appears-google-earth-123066>

"Google's Chiller-less Data Center » Data Center Knowledge", Data Center Knowledge, online: <http://www.datacenterknowledge.com/archives/2009/07/15/googles-chiller-less-data-center/>

"Black Friday traffic takes down Sears.com", msnbccom, online: <http://www.msnbc.msn.com/id/27957529/ns/technology_and_science-tech_and_gadgets/t/black-friday-traffic-takes-down-searscom/>

"GCHQ: Big Brother plans to let state spy on websites, emails and texts to cost YOU £2bn", Mail Online, online: <http://www.dailymail.co.uk/news/article-2124251/GCHQ-Big-Brother-plans-let-state-spy-websites-emails-texts-cost-YOU-2bn.html>

Ackermann, Timothy G. Consent and Discovery Under the Stored Communications Act (2009)

Armbrust, Michael et al. Above the Clouds: A Berkeley View of Cloud Computing (Berkeley: University of California at Berkeley, 2009)

Armstron, Jonathan P & Eberhard H Rohm. Data Protection Regulator for Germany's Schleswig-Holstein Calls for European Review of FTC's Safe-Harbor Program (2010)

Article 2 Working Party. Working Document on Determining the International Application of EU data protection law to personal data processing on the Internet by non-EU based web sites (Brussels: Article 29 Working Party, 2002)

Article 29 Working Party. Opinion 1/2008 on data protection issues related to search engines (Brussels: Article 29 Working Party, 2008)

Article 29 Working Party. Working Document 1/2009 on pre-trial discovery for cross border civil litigation (Brussels: Article 29 Working Party, 2009)

Article 29 Working Party. Opinion 5/2009 on Online Social Networking (Brussels: Article 29 Working Party, 2009)

Article 29 Working Party. Opinion 8/2010 on applicable law (Brussels: Article 29 Working Party, 2010)

Article 29 Working Party. Opinion 1/2010 on the concepts of "controller" and "processor" (Brussels: Article 29 Working Party, 2010)

Asia Cloud Forum Staff. "China builds 10 sq km cloud computing special zone in Chongqing | Asia Cloud Forum", (2 March 2011), online: <http://www.asiacloudforum.com/content/china-builds-10-sq-km-cloud-computing-special-zone-chongqing>

Ballmer, Steve. Cloud Computing (Paul G. Allen Center for Computer Science & Engineering, University of Washington, 2010)

Barlow, John Perry. "A Declaration of the Independence of Cyberspace", (8 February 1996), online: Electronic Frontier Foundation <https://projects.eff.org/~barlow/Declaration-Final.html>

Black, Jay. "Don't Cloud SFU Data", (3 February 2012), online: Jay Black's CIO Blog, Simon Fraser University <http://www.sfu.ca/itservices/about/depts/cio/cioblog/2012/02/dont_cloud_sfu_data.html>

Boutelle, Jonathan. "How Cloud Computing Impacts the Cash Needs of Startups", (16 August 2010), online: GigaOM <http://gigaom.com/cloud/how-computing-impacts-the-cash-needs-of-startups/>

Bradshaw, Simon, Christopher Millard & Ian Walden. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services (London: Queen Mary University of London, School of Law, 2010)

Brodkin, Jon. "Microsoft: We make more money on cloud-based Exchange | Asia Cloud Forum", (16 August 2011), online: Asia Cloud Forum <http://www.asiacloudforum.com/content/microsoft-we-make-more-money-cloud-based-exchange>

Camin, Cheryl S. "HIPAA: To Preempt or Not To Preempt? That is the Question (Especially in Litigation)", (2005), online: ABA Health eSource <http://www.americanbar.org/newsletter/publications/aba_health_esource_home/Volume2_vol2no1_camin.html>

Cate, Fred H. Provincial Canadian Geogrpahical Restrictions on Personal Data in the Public Sector (Washington, DC: The Center for Information Policy Leadership, 2008)

Catteddu, Daniel & Giles Hogben. Cloud Computing: Benefits, risks and recommendations for information security (European Network and Information Security Agency, 2009)

Chander, Anupam. Who Shall Govern the Cloud? (University of Toronto Faculty of Law, 2011)

Choo, Kim-Kwang Raymond. Cloud computing: Challenges and future directions (Canberra: Australian Government, Australian Institute of Criminology, 2010)

Clinton, William J & Albert Gore. The Framework for Global Electronic Commerce (Washington, DC: The White House, 1997)

CNIL. Deliberation no. 2011-023 (CNIL, 2011)

CNIL. Google's new privacy policy raises deep concerns about data protection and the respect of the European law (Paris: CNIL, 2012)

Convery, Nicole. Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud (Department of Information Studies, Aberystwyth University, 2010)

Crossman, Penny. "Fieldpoint Private Bank Turns to Cloud Computing for CRM and Beyond - Bank Systems & Technology",, online: Banktechcom <http://www.banktech.com/business-intelligence/225702942>

Doyle, Charles. The USA PATRIOT ACT: A Legal Analysis (Washington, DC: Congressional Research Service, 2002)

European Commission. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Brussels: European Commission, 2012)

Falque-Pierrotin, Isabelle. CNIL Letter to Google (CNIL, 2012)

Filnet. "Microsoft 365 et Patriot Act: Filnet appelle les entreprises à choisir un Cloud Made In France | Filnet", (Juillet 2011), online: Filnetfr <http://www.filnet.fr/content/microsoft-365-et-patriot-act-filnet-appelle-les-entreprises-choisir-un-cloud-made-france>

Fraser, David TS. "Canadian Privacy Law Blog: Patriot Act reality check and Canadian authorities' similar powers", (28 April 2010), online: Canadian Privacy Law Blog <http://blog.privacylawyer.ca/2010/04/patriot-act-reality-check-and-canadian.html>

Fraser, David TS. The Cloud Thing: Privacy and cloud computing (Dalhousie U. Halifax, N.S., 2011)

Fraser, David TS. "Canadian Privacy Law Blog: Cloud Computing and Privacy FAQ", (18 April 2011), online: Canadian Privacy Law Blog <http://blog.privacylawyer.ca/2011/04/cloud-computing-and-privacy-faq.html>

Galperin, Eva. "What Does Twitter's Country-by-Country Takedown System Mean for Freedom of Expression?", (27 January 2012), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2012/01/what-does-twitter%E2%80%99s-country-country-takedown-system-mean-freedom-expression>

Geist, Michael. "Michael Geist - SOPA: All Your Internets Belong to US", (16 November 2011), online: <http://www.michaelgeist.ca/content/view/6134/135/>

Google. Google Contribution to the Public Consultation on Cloud Computing (Brussels, 2011)

Google France SARL. Google France Letter to CNIL, April 5, 2012 (Google France SARL, 2012)

Google Inc. "Google Accounts", (2012), online: Google <https://www.Google.com/dashboard>

Heiliger, Jonathan. "Breaking Ground on Our First Custom Data Center", (21 January 2010), online: Facebook <http://blog.facebook.com/blog.php?post=262655797130>

Hon, W Kuan, Christopher Millard & Ian Walden. Who is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2 (London: Queen Mary University of London, School of Law, 2011)

Jaeger, Paul et al. "Where is the cloud? Geography, economics, environment and jurisdiction in cloud computing", (May 2009), online: First Monday <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171>

Kennedy, The Rt Hon Sir Paul. 2010 Annual Report of the Interception of Communications Commissioner (Parliament of the United Kingdom, 2011)

Kerr, Orin. A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It (Washington, DC: George Washington University Law School, 2004)

Klein, Kris. Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act: Transborder Data Flows and their Regulation (Law Office of Kris Klein for Salesforce.com, 2010)

Knights, Miya. "Memset signs up as provider for government cloud initiative", (27 September 2011), online: Cloud Pro <http://www.cloudpro.co.uk/cloud-essentials/public-cloud/1797/memset-signs-provider-government-cloud-initiative>

Kroes, Neely. EUROPA - Press Releases - Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Ending fragmentation of the Digital Single Market Business For New Europe event London, 7 February 2011 (London, 2011)

Kundra, Vivek. The Shift to Cloud Computing (Washington, DC, 2010)

Legal Cloud Computing Association. Response to North Carolina State Bar Proposed 2011FEO6 - Legal Cloud Computing Association (Legal Cloud Computing Association, 2011)

Lord Neuberger. Report of the Committee on Super-Injunctions: Super-Injunctions, Anonymised Injunctions and Open Justice (London: Judiciary of England and Wales, 2011)

Lynsky, Orla, Neil Robinson & Michael Greenberg. e-Discovery and legal frameworks covering Privacy and Data Protection in European countries (RAND Europe, 2010)

Mell, Peter & Timothy Grace. The NIST Definition of Cloud Computing (Washington, DC: National Institute of Standards and Technology, 2011)

Microsoft. Microsoft's Response to the Commission's Public Consultation on Cloud Computing (Brussels: Microsoft, 2011)

National Association of Attorneys General. National Association of Attorneys General letter of Feb. 22, 2012 to Larry Page of Google, Inc. (National Association of Attorneys General, 2012)

Neily, Katelyn E. "Orato: UBC Student Data Illegally Stored in US BC's FIPPA Law Bans Turitin Plagiarism Check", (18 March 2012), online: Orato <http://www.orato.com/tech-games/ubc-student-data-illegally-stored-us>

Neuburger, Jeffrey D & Natalie Newman. The Bay State Raises the Bar on Personal Data Security: Are You in Compliance? (Washington, DC: Washington Legal Foundation, 2010)

Obama, Barrack. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (The White House, 2012)

Sedlarcik, Frank P & Nancy L Hoffman. Litigating at Home and Fact Finding Abroad (American Intellectual Property Law Association)

Smith, Brad. Remarks by Brad Smith, General Counsel and Senior Vice President, Legal and Corporate Affairs (National Assembly, Paris, 2011)

Soghoian, Christopher. "slight paranoia: How long does it take for the FTC to investigate a company?", (February 2012), online: Slight Paranoia <http://paranoia.dubfire.net/2012/02/how-long-does-it-take-for-ftc-to.html>

Soghoian, Christopher. "Twitter's privacy policy and the Wikileaks case",, online: <http://paranoia.dubfire.net/2011/11/twitters-privacy-policy-and-wikileaks.html>

Stoddard, Jennifer. "Commissioner's Findings - PIPEDA Case Summary #394: Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers (August 7, 2008)", (2008), online: <http://www.priv.gc.ca/cf-dc/2008/394_20080807_e.cfm>

US Immigration and Customs Enforcement. "Operation In Our Sites protects American online shoppers, cracks down on counterfeiters", (28 November 2011), online: ICEgov <http://www.ice.gov/news/releases/1111/111128washingtondc.htm>

Veld, Sophia in 't. "Written question - Access to EU data by US authorities - E-006901/2011", (13 July 2011), online: Europarl <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-006901+0+DOC+XML+V0//EN>

Wagner, Ben. Deep Packet Inspection and Internet Censorship: International Convergence on an "Integrated Technology of Control" (Global Voices Advocacy)

Wikipedia contributors. Sneakernet (Wikimedia Foundation, Inc., 2012)

Wikipedia contributors. Netflix (Wikimedia Foundation, Inc., 2012)

Wikipedia contributors. List of Google products (Wikimedia Foundation, Inc., 2012)

Yoo, Christopher S. Cloud Computing: Architectural and Policy Implications (Philadelphia: University of Pennsylvania, 2011)

Zetter, Kim. "FBI Defends Disruptive Raids on Texas Data Centers", (April 2009), online: WIRED <http://www.wired.com/threatlevel/2009/04/data-centers-ra/>

Ziervogel, Jan. "The Natural Location for a Data Centre", (2012), online: <http://www.greendataisland.com/Volcanoes.html>

"Google Health and HIPAA",, online: Google Health <http://www.google.com/intl/en_us/health/hipaa.html>

Restatement of the Foreign Relations Law of the United States, Third (1987) (Philadelphia: American Law Institute, 1987)

"Preemption by/of state laws (HIPAA)", (2005 2002), online: University of Miami, Miller School of Medicine Privacy / Data Protection Project <http://privacy.med.miami.edu/glossary/xd_state_preemption.htm>

The Hague Convention of 20 June 2005 on Choice of Court Agreements (2005)

"In the Matter of Superior Mortgage Corp., File No. 052 3136 (Consent Order)", (28 September 2005), online: Federal Trade Commission <http://www.ftc.gov/os/caselist/0523136/0523136.shtm>

"Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule", (7 September 2006), online: Federal Trade Commission <http://www.ftc.gov/opa/2006/09/xanga.shtm>

"UMG Recordings, Inc. to Pay $400,000, Bonzi Software, Inc. To Pay $75,000 to Settle COPPA Civil Penalty Charges", (13 September 2006), online: Federal Trade Commission <http://www.ftc.gov/opa/2004/02/bonziumg.shtm>

"How to Comply with the Children's Online Privacy Protection Rule | BCP Business Center", (December 2006), online: Federal Trade Commission Bureau of Consumer Protection <http://business.ftc.gov/documents/bus45-how-comply-childrens-online-privacy-protection-rule>

"HIPAA Privacy Rule and Its Impacts on Research", (2 February 2007), online: US Dept of Health and Human Services, National Institutes of Health <http://privacyruleandresearch.nih.gov/pr_06.asp>

"Google limits the search data retention period", (28 March 2007), online: EDRI Digital Civil Rights in Europe <http://www.edri.org/edrigram/number5.6/google-data-retention>

"How long should Google remember searches?", (12 June 2007), online: Google Official Blog <http://googleblog.blogspot.ca/2007/06/how-long-should-google-remember.html>

Cloud Computing (Computer and Communications Industry Association, 2009)

Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) In Support of Appellee and Urging Affirmance, Sorrell v. IMS (Electronic Information Privacy Center, 2009)

"Google: China is messing with Gmail - Google 24/7 - Fortune Tech", (2010), online: <http://tech.fortune.cnn.com/2011/03/21/google-china-is-messing-with-gmail/>

"Digital Due Process: Modernizing Surveillance Laws for the Internet Age", (2010), online: Digital Due Process <http://digitalddueprocess.org/index.cfm?objectid=FE5C92F0-2552-11DF-B455000C296BA163>

Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing (Microsoft, 2010)

Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing (Microsoft, 2010)

"Official Google Blog: Serious threat to the web in Italy", (24 February 2010), online: <http://googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html>

Official Google Enterprise Blog: An update for our customers on Google Apps and China (2010)

"Cloud Computing in the EU: Getting a grip on the data protection/data security issues", (13 September 2010), online: Project Counsel <http://www.projectcounsel.com/?p=646>

Cloud Legal Project response to European Commission Cloud Computing Consultation, Queen Mary, University of London (London, 2011)

"Forrester's Global Data Protection and Privacy Heatmap", (2011), online: Forrester Tools <http://heatmap.forrestertools.com/>

Processing of sensitive personal data in a cloud solution (Datatilsynet, 2011)

"Department of Commerce Official Asks Congress to Enact 'Privacy Bill of Rights'", (16 March 2011), online: Privacy and Information Security Law Blog <http://www.huntonprivacyblog.com/2011/03/articles/department-of-commerce-official-asks-congress-to-enact-privacy-bill-of-rights/>

"FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network; Google Agrees to Implement Comprehensive Privacy Program to Protect Consumer Data", (30 March 2011), online: Federal Trade Commission <http://www.ftc.gov/opa/2011/03/google.shtm>

"John Kerry - United States Senator for Massachusetts : At Work for You in Congress - List of All Issues - Commercial Privacy Bill of Rights", (12 April 2011), online: Kerrysenategov <http://kerry.senate.gov/work/issues/issue/?id=74638d00-002c-4f5e-9709-1cb51c6759e6&CFID=79733731&CFTOKEN=26547080>

"EUROPA - Press Releases - Viviane Reding Vice-President of the European Commission, EU Justice Commissioner The reform of the EU Data Protection Directive: the impact on businesses European Business Summit Brussels, 18 May 2011", (18 May 2011), online: Europa <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/349&format=HTML&aged=1&language=EN&guiLanguage=en>

"How Would the Kerry-McCain 'Commercial Privacy Bill of Rights' Affect State Security and Privacy Laws?", (20 May 2011), online: Electronic Frontier Foundation <https://www.eff.org/deeplinks/2011/05/how-would-kerry-mccain-commercial-privacy-bill>

"Microsoft's Office 365 Cloud Service Goes Live Worldwide - Microsoft in Health - Site Home - MSDN Blogs", (28 June 2011), online: MSDN

<http://blogs.msdn.com/b/microsoft_in_health/archive/2011/06/28/microsoft-s-office-365-cloud-service-goes-live-worldwide.aspx>

Motion to dismiss, in the matter of Google v. United States, in the United States Court of Federal Claims (Google Inc., 2011)

Judgment in Case C-70/10: Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Court of Justice of the European Union, 2011)

"Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises", (29 November 2011), online: <http://ftc.gov/opa/2011/11/privacysettlement.shtm>

Report of Data Protection Audit of Facebook Ireland (Dublin: Data Protection Commission, Ireland, 2011)

"AWS GovCloud (US)", (2012), online: Amazon Web Services <http://aws.amazon.com/govcloud-us/>

"iOS Dev Center", (2012), online: Apple Developer <http://developer.apple.com/devcenter/ios/index.action>

"Twitter Help Center, Guidelines for Law Enforcement", (2012), online: Twitter <https://support.twitter.com/articles/41949-guidelines-for-law-enforcement>

"Data Liberation Front", (2012), online: Google <http://www.dataliberation.org/>

"State Laws Related to Internet Privacy", (2012), online: National Conference of State Legislatures <http://www.ncsl.org/issues-research/telecom/state-laws-related-to-internet-privacy.aspx>

"Safe Harbor - List", (2012), online: Exportgov <https://safeharbor.export.gov/list.aspx>

"Pandora", (2012), online: Pandora <http://www.pandora.com>

"Mapping Local Internet Control - GeoMap Visualization Demo", (2012), online: Berkman Center for Internet & Society at Harvard University <http://cyber.law.harvard.edu/netmaps/geo_map_home.php>

"MegaRetrieval", (2012), online: <http://megaretrieval.com/>

Indictment: United States of America v. Kim Dot Com, Megaupload, Inc., et. al. (United States District Court for the Eastern District of Virginia, Alexandria Division, 2012)

Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (Washington, DC: Federal Trade Commission, 2012)

Registration Statement on Form S-1, filed with United States Seccurities and Exchange Commission (Facebook, 2012)

"State Security Breach Notification Laws", (6 February 2012), online: National Conference of State Legislatures <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>

"Kerry Statement on Obama Privacy Bill of Rights", (23 February 2012), online: Kerrysenategov <http://kerry.senate.gov/press/release/?id=36D3DCC0-9FD8-4A0A-BA5B-ED411C97E108>

"Google Terms of Service – Policies & Principles", (March 2012), online: Google <http://www.google.com/intl/en/policies/terms/>

"Salesforce", (9 April 2012), online: Salesforce <http://www.salesforce.com/>

"Amazon Web Services",, online: <http://aws.amazon.com/>

"Google Apps for Business | Official Website",, online: <http://www.google.com/apps/intl/en/business/index.html>

"Google App Engine — Google Developers",, online: <https://developers.google.com/appengine/>

"Google Fiber & Kansas City",, online: <http://www.google.com/fiber/kansascity/about.html>

"Google Data Center Locations",, online: Google <http://www.google.com/about/datacenters/locations/index.html>

"NAP of the Americas, South Florida Data Center, Tier IV Facility, Terremark",, online: Terremark <http://www.terremark.com/technology-platform/nap-of-the-americas.aspx>

U.S. Federal Rule of Civil Procedure 26(b)(1)

"Google Terms of Service – Policies & Principles – (Former version dated April 16, 2007)",, online: <http://www.google.com/intl/en/policies/terms/archive/20070416/>

"In the Matter of Superior Mortgage Corp., File No. 052 3136",, online: Federal Trade Commission <http://www.ftc.gov/os/caselist/0523136/0523136.shtm>

"List of Internet top-level domains - Wikipedia, the free encyclopedia",, online: <http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains#USA_top-level_domains>

"DIFC Data Protection Law",, online: <http://dp.difc.ae/>