**Northwestern Journal of Technology and Intellectual Property**

Volume 9
Issue 2 *November*

Article 2

Fall 2010

# Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?

Paul Lanois

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

# Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?

*Paul Lanois*


November 2010 VOL. 9, NO. 2

Northwestern Journal of Technology and Intellectual Property
Volume 9, Number 2 (November 2010)

# Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?

**By Paul Lanois***

## I. INTRODUCTION

¶1 According to a recent study by The Nielsen Company, the average American Internet user spends over fifty-five hours per month online.[1] However, despite the wide range of possibilities offered by the Internet, Americans spend about half of their online time on social networks, games, e-mail, and instant messaging.[2] As consumers are spending an increasing amount of time online and demanding convenient, instant access to more content, cloud computing is becoming a rapidly growing technology and the industry's new buzzword.[3] In a nutshell, the idea behind cloud computing is that instead of having the software and data stored locally on a user's own computer, they can all be stored on Internet servers, or "in the clouds," and accessed as a service on the Internet.

¶2 Thanks to cloud computing, users no longer have to worry about storage capacity, memory, endless hardware purchases and upgrades, lengthy software downloads, or constant updates.[4] This is because applications all run directly from the cloud, not from

---

* Paul Lanois is an Associate Professor at the University of Cergy-Pontoise (France) and Attorney at Law of the New York Bar. He was previously an associate at Simpson Thacher & Bartlett LLP in London, United Kingdom. He graduated from the University of Paris–Sorbonne (France) with a Master's degree in Business Law and a postgraduate degree in Private and Public Economic Law, and holds an LL.M. degree from the University of Pennsylvania Law School.

[1] *See* Nielsen, *June 2010: Top Online Sites and Brands in the U.S.*, NIELSEN WIRE (July 16, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/june-2010-top-online-sites-and-brands-in-the-u-s/ (The study also found that the average time spent online in the U.S. grew by more than 3% in July 2010 compared to June 2010, and includes both home and work usage of the Internet.).

[2] *See* Nielsen, *What Americans Do Online: Social Media And Games Dominate Activity*, NIELSEN WIRE (Aug. 2, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity/ (The study tracked the online activity of 200,000 American users from June 2009 to June 2010.).

[3] *See, e.g.*, Margaret Lewis, *Cloud Computing: Hype Vs. Reality*, FORBES.COM (Aug. 03, 2010, 12:00 PM), http://www.forbes.com/2010/08/03/open-source-virtualization-technology-cloud-computing.html; Janna Q. Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW INTERNET & AMERICAN LIFE PROJECT (June 11, 2010), http://pewresearch.org/pubs/1623/future-cloud-computing-technology-experts; Galen Gruman & Eric Knorr, *What Cloud Computing Really Means*, INFOWORLD.COM (Apr. 07, 2008, 3:00 AM), http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031; Rachael King, *How Cloud Computing Is Changing the World*, BLOOMBERG BUSINESSWEEK (Aug. 04, 2008, 12:01 AM), *available at* http://www.businessweek.com/print/technology/content/aug2008/tc2008082_445669.htm; Chloe Albanesius & Mark Hachman, *Microsoft Betting Its Future on Cloud Computing*, PCMAG.COM (Mar. 04, 2010), http://www.pcmag.com/article2/0,2817,2360963,00.asp; Joshua Brockman, *Counting On The Cloud To Drive Computing's Future*, NATIONAL PUBLIC RADIO (Mar. 27, 2009), http://www.npr.org/templates/story/story.php?storyId=102453091.

[4] *See, e.g.*, Bernard Golden, *How Cloud Computing Can Transform Business*, HARVARD BUS. REV. (June 04, 2010), *available at* http://blogs.hbr.org/cs/2010/06/business_agility_how_cloud_com.html; Michael Miller, *Cloud Computing Pros and Cons for End Users*, INFORMIT (Feb. 13, 2009),

the user's desktop computer; therefore, the computer does not need to have the same processing horsepower or hard disk space typically required by traditional software. Since the software and data are entirely web-based, the user automatically has access to the latest version of the program wherever he or she is located, without having to bring the data or software. In addition, users are not tied to specific devices or network interfaces in order to use an application,[5] thus eliminating compatibility issues and the need for software developers to create specific versions of the application for each device.

¶3 Due to the significant benefits offered by cloud computing, a large number of companies have been eager to hop on the cloud bandwagon. Hardware makers, software giants, and service providers alike have already released offerings such as: Amazon's Elastic Compute Cloud,[6] Microsoft's Cloud Services and Windows Azure,[7] AT&T's Cloud Services,[8] Hewlett-Packard's Cloud Assure[9] and Cloud Consulting Services,[10] IBM's Smart Business Storage Cloud[11] and Smart Analytics Cloud,[12] VMware's vCloud,[13] or Logica's Cloud Services.[14] The uptake of cloud computing is such that some believe a wide-scale adoption of cloud computing will occur in the near future. Information technology (IT) research and advisory company Gartner, Inc. already forecasts the market for cloud services to significantly expand in the coming years, from $58.6 billion in revenues in 2009 to an estimated $68.3 billion in 2010 and $148.8 billion in 2014.[15] Likewise, another IT research and analysis firm, International Data Corporation (IDC), already forecasts that the spending by IT organizations on cloud servers will grow by over 20% by 2014, from $582 million in 2009 to $718 million in 2014.[16] The recent bidding war between Hewlett-Packard and Dell to acquire cloud storage firm 3PAR serves as an illustration that the interest in cloud computing and confidence in its growth is strong.[17]

---

http://www.informit.com/articles/article.aspx?p=1324280.

[5] Golden, *supra* note 4; Miller, *supra* note 4.

[6] *Amazon Elastic Compute Cloud (Amazon EC2)*, AMAZON WEB SERVS., http://aws.amazon.com/ec2/ (last visited Nov. 6, 2010).

[7] *Microsoft Cloud Services*, MICROSOFT, http://www.microsoft.com/cloud/ (last visited Nov. 6, 2010).

[8] *Extend Your Reach with AT&T Cloud Services*, AT&T, http://www.business.att.com/enterprise/online_campaign/cloud_computing (last visited Nov. 6, 2010).

[9] Press Release, HP, *HP Unveils "Cloud Assure" to Drive Business Adoption of Cloud Services* (Mar. 31, 2009), http://www.hp.com/hpinfo/newsroom/press/2009/090331xa.html.

[10] *HP Cloud Consulting Services*, HP, http://h20219.www2.hp.com/services/us/en/consolidated/cloud-overview.html (last visited Nov. 6, 2010).

[11] *Smart Business Storage Cloud*, IBM, http://www-935.ibm.com/services/us/index.wss/offering/its/a1031610 (last visited Nov. 6, 2010).

[12] *Smart Analytics Cloud for System Z*, IBM, http://www-03.ibm.com/systems/z/solutions/cloud/smart.html (last visited Nov. 6, 2010).

[13] *VMware vCloud*, VMWARE, http://www.vmware.com/products/vcloud/ (last visited Oct. 3, 2010).

[14] *Cloud Services*, LOGICA, http://www.logica.com/we-do/future%20it%20and%20cloud%20services/cloud%20services/ (last visited Oct. 3, 2010).

[15] Press Release, Gartner, Inc., *Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010* (June 22, 2010), http://www.gartner.com/it/page.jsp?id=1389313.

[16] *See* Anton Shilov, *Cloud Computing to Drive $6.4 Billion in Server Hardware Spending by 2014 - Analyst*, XBITLABS (Aug. 09, 2010, 9:06 PM), http://www.xbitlabs.com/news/other/display/20100809210619_Cloud_Computing_to_Drive_6_4_Billion_in_Server_Hardware_Spending_by_2014_Analyst.html.

[17] Rick Merritt, *How 3Par Became a $2 Billion Company*, EE TIMES (Aug. 27, 2010, 3:56 PM),

¶4 Of course, cloud computing is not solely restricted to the IT industry or a work environment, as it has already began penetrating the mainstream market. Since consumers are spending an increasing amount of their time on online games, surpassing even e-mailing in terms of time spent,[18] it is not surprising to see startups working on new gaming solutions based on the cloud.[19] For instance, cloud gaming services such as OnLive[20] or Gaikai[21] are promising to disrupt the gaming industry by delivering the latest high-end video games through the cloud to a computer or even an Internet-connected device.[22] Some analysts are already predicting that the days of traditional, casual gaming may soon be over, with cloud-based gaming set to take its place by sweeping away the hurdles that make setting up and playing games a hassle for many users.[23] These services work by handling the intensive game processing on the cloud servers; since only the video feed is streamed to the user's computer this enables users to play games with high-end visuals without the need for expensive hardware (such as the latest and greatest graphics cards or processors) in their system.[24] Despite having launched its service only in June 2010,[25] OnLive is already said to be worth at least $1.1 billion after receiving investments from British Telecommunications (BT) and the Belgacom Group.[26] Cloud computing is also poised to reshape the media industry. The Digital Entertainment Content Ecosystem (DECE), a cross-industry consortium that includes sixty technology and entertainment companies, has announced their plan to launch "UltraViolet," a cloud-based user management system which will allow users to buy digital content from a provider, store it in a "digital locker," and watch it across multiple platforms such as

---

http://www.eetimes.com/electronics-news/4206551/How-3Par-became-2-billion-company ("How can a company that has never shown a profit and had flat 2010 revenues of less than $200 million suddenly become worth $2 billion? That's the story of the 3Par bidding war, and it speaks volumes about the dynamics of today's computer industry."); Rolfe Winkler, *H-P Pushes 3PAR Price to the Clouds*, WALL ST. J. (Aug. 24, 2010), *available at* http://online.wsj.com/article/SB10001424052748703846604575447731336631668.html; Rob Enderle, *3Par: First Pivotal Battle Between Dell and HP*, TG DAILY (Aug. 27, 2010, 1:54 PM), http://www.tgdaily.com/opinion/51291-3par-first-pivotal-battle-between-dell-and-hp.

[18] *See* Nielsen, *supra* note 2.

[19] *See* Paul Lanois, *Gaming and Digital Rights Management Reaching for the Clouds*, INT'L INTELL. PROP. & RELATED LEGAL ISSUES IN VIRTUAL WORLDS, A.B.A. (forthcoming 2011).

[20] John Biggs, *OnLive Cloud Gaming Service Goes Live June 17*, TECHCRUNCH (June 15, 2010), http://techcrunch.com/2010/06/15/onlive-cloud-gaming-service-goes-live-june-17/; Pulkit Chandn, *OnLive's Cloud-Gaming Service to Launch Thursday*, MAXIMUM PC (June 15, 2010, 6:26 PM), http://www.maximumpc.com/article/news/onlives_cloudgaming_service_launch_thursday; Chris Baker, *OnLive's 'Cloud Gaming' Could Be a Game-Changer*, WIRED (Mar. 24, 2009), *available at* http://www.wired.com/gamelife/2009/03/cloud-gaming.

[21] *See, e.g.*, Dean Takahashi, *Game-streaming Firm Gaikai Raises Funding from Intel Capital and Limelight Networks*, VENTURE BEAT (July 20, 2010), http://games.venturebeat.com/2010/07/20/game-streaming-firm-gaikai-raises-funding-from-intel-capital-and-limelight-networks/; Dean Takahashi, *Gaikai Signs EA as Digital Distribution Partner*, VENTURE BEAT (June 17, 2010), http://games.venturebeat.com/2010/06/17/gaikai-signs-ea-as-digital-distribution-partner/.

[22] *See* Lanois, *supra* note 19.

[23] *See* Christopher Dring, *EEDAR: Cloud Gaming Could Kill Farmville*, MCV (Aug. 16, 2010), *available at* http://www.mcvuk.com/news/40448/EEDAR-Cloud-gaming-could-kill-Farmville.

[24] *See* Lanois, *supra* note 19.

[25] *See* Lanois, *supra* note 19.

[26] Dean Takahashi, *Online Game Service OnLive's Latest Filing Points to $1.1 Billion Valuation*, VENTURE BEAT (Aug. 04, 2010), http://games.venturebeat.com/2010/08/04/online-game-service-onlives-latest-filing-points-to-1-1-billion-valuation/.

connected TVs, PCs, game consoles, and smart phones.[27] The Walt Disney Company is also working on a similar cloud-based digital locker technology, dubbed "Keychest."[28]

¶5 Last but not least, the Ford Motor Company is developing a new system that could bring cloud computing and social networking features to the upcoming range of cars. [29] The research project, led by Ford Motor's Research and Advanced Engineering program in partnership with students from the University of Michigan, could shape the future of in-car connectivity by harnessing "the power of social networks and cloud computing"[30] to deliver personalized content and improve users' experiences. The applications developed feature real-time fuel consumption monitoring, GPS location awareness, traffic alerts, routes and points-of-interest sharing, and include tools allowing drivers to stay connected with each other by sharing information such as their locations, direction, fuel level, and speed, as well as sending notifications to others about road conditions and hazards.[31] These examples illustrate the tremendous possibilities of cloud computing and its potential for growth as we move into an increasingly digital and connected world. However, the increase in the number of connected devices, such as smart phones[32] and new tablet computers, combined with the significant growth of social networking and cloud computing, have also created privacy loopholes and security threats.

## II. PRIVACY IN A DIGITAL WORLD AND THE USE OF COOKIES

¶6 Consumers and businesses alike are increasingly taking advantage of the possibilities offered by cloud computing and are already storing their private emails, photos, videos, files, and other data on the Internet instead of their own personal computer, thanks to online, cloud-based services such as Gmail,[33] Google Docs,[34]

---

[27] *See* Lanois, *supra* note 19; *see also* Ryan Nakashima, *UltraViolet Digital Movie Locker Would Let You Play Movies Anywhere*, THE HUFFINGTON POST (July 20, 2010, 6:38 PM), http://www.huffingtonpost.com/2010/07/20/ultraviolet-movie-locker-_n_652396.html; *see also* Press Release, Digital Entertainment Content Ecosystem LLC, *Digital Entertainment Content Ecosystem Unveils UltraViolet Brand* (July 20, 2010), http://www.uvvu.com/press/UltraViolet_Brand_Launch_Release_07_20_2010_FINAL.PDF.

[28] *See* Lanois, *supra* note 19; *see also* Ethan Smith, *Disney Touts a Way to Ditch the DVD*, WALL ST. J. (Oct. 21, 2009), *available at* http://online.wsj.com/article/SB10001424052748703816204574485650026945222.html.

[29] *See* Ford Motor Co., *Ford and U-M Use Socially Connected Road Trip to Debut Car as Next Platform for Cloud Computing* (May 12, 2010), http://media.ford.com/article_display.cfm?article_id=32623; Ford Motor Co., *Ford, University of Michigan Reveal Students' Vision for Future of In-Car Cloud Computing Apps* (May 04, 2010), http://media.ford.com/article_display.cfm?article_id=32572.

[30] *See Ford and U-M Use Socially Connected Road Trip to Debut Car as Next Platform for Cloud Computing*, *supra* note 29; *Ford, University of Michigan Reveal Students' Vision for Future of In-Car Cloud Computing Apps*, *supra* note 29.

[31] *See Ford and U-M Use Socially Connected Road Trip to Debut Car as Next Platform for Cloud Computing*, *supra* note 29; *Ford, University of Michigan Reveal Students' Vision for Future of In-Car Cloud Computing Apps*, *supra* note 29.

[32] *See* Press Release, comScore, Inc., *comScore Reports February 2010 U.S. Mobile Subscriber Market Share - Use of Social Media via Mobile Device Continues to Post Strong Gains* (Apr. 05, 2010), http://www.comscore.com/Press_Events/Press_Releases/2010/4/comScore_Reports_February_2010_U.S._Mobile_Subscriber_Market_Share.

[33] Stephen Wildstrom, *Cloud Computing: Understand the Risks*, BLOOMBERG BUSINESSWEEK (Mar. 25, 2009), *available at* http://www.businessweek.com/magazine/content/09_14/b4125000676483.htm.

[34] *Id.*

Flickr,[35] Picasa,[36] and YouTube.[37] Services such as popular social networking sites Facebook and Twitter also make use of cloud computing.[38] However, protecting the identity of consumers in the digital world is proving to be quite a challenge, as shown by the controversies surrounding Facebook's privacy settings,[39] Google's accidental capturing of some Internet users' unencrypted Wi-Fi traffic,[40] and even the hacking attacks on Twitter[41] or Google's Gmail service.[42]

¶7 Previously, the monitoring of a user's browsing habits was done through the use of a computer "cookie," which is a small file of letters and numbers that acts as an identifier on a website. Cookies allow the website server that sent the cookie and stored it as a file on the user's computer to recognize the user when he or she returns to the site, and also to track his or her web usage.[43] Cookies are thus a way of storing user information on the user's computer so that the site may access and maintain information on the user whenever he or she connects to the site. For instance, a cookie can be used to save your login name, your preferences for viewing content, or to track you as you browse the Internet. Cookies are of particular interest to online advertising firms since the cookies can be used to gather information on the user's Internet habits and to display online advertisements targeted at a specific user based on his or her browsing habits. For example, the Wall Street Journal recently found that a cookie file containing a single line of code can be used to trace the activities of the user and identify her age, town, and even her favorite movies.[44] However, advertising is not the only purpose of cookies. Cookies are also used to store information on behalf of the user, such as a user's website preferences or the contents of an online shopping cart. If a user fills out an internet form with her name, address, and other personal information, cookies may be used to store this information so that the next time the same user visits the site, the information is automatically provided to the website and the user does not have to provide it again. In particular, cookies are relevant to cloud computing since cookies are used for authentication purposes, such as identifying a server-based session, or storing and

---

[35] *Id.*

[36] Stephen Shankland, *Google Gives Picasa 3.8 a Cloud Connection*, CNET NEWS (Aug. 18, 2010, 12:46 PM), http://news.cnet.com/8301-30685_3-20014029-264.html.

[37] *See* Kyle VanHemert, *YouTube Gets Simple, Cloud-Based Video Editing*, GIZMODO (June 16, 2010, 4:40 PM), http://gizmodo.com/5565329/youtube-gets-simple-cloud+based-video-editing.

[38] *See* Anderson & Rainie, *supra* note 3.

[39] *See* Jon Swartz, *Facebook Draws Protests on Privacy Issue*, USA TODAY (May 13, 2010), *available at* http://www.usatoday.com/money/media/2010-05-14-facebook14_ST_N.htm; Jessica E. Vascellaro, *Facebook Grapples With Privacy Issues*, WALL ST. J. (May 19, 2010), *available at* http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748704912004575252723109845974.html; Caroline McCarthy, *Do Facebook's New Privacy Settings Let it off the Hook?*, CNET NEWS (May 26, 2010, 12:07 PM), http://news.cnet.com/8301-13577_3-20006054-36.html.

[40] *See* Cecilia Kang, *Lawmakers Press FTC on Google Street View Privacy Lapse*, WASH. POST (May 19, 2010), *available at* http://voices.washingtonpost.com/posttech/2010/05/us_lawmakers_press_ftc_on_inve.html.

[41] *See* Press Release, Fed. Trade Comm'n Office of Public Affairs, *Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program* (June 24, 2010), http://www.ftc.gov/opa/2010/06/twitter.shtm.

[42] *See Google 'May Pull Out of China After Gmail Cyber Attack'*, BBC NEWS (Jan. 13, 2010, 11:38 PM), http://news.bbc.co.uk/2/hi/business/8455712.stm.

[43] *See* Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010), *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[44] *Id.*

maintaining login and password information or similar data, administering the user's account, or identifying the browser used.

¶8 In order to gain a better understanding of the extent of the monitoring and its impact on privacy, the Wall Street Journal recently conducted an investigation and found that "the nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning."[45] The investigation also found that the information collected on users is constantly updated and compiled into specific user profiles, which are then "bought and sold on stock market-like exchanges."[46]

¶9 In addition, the monitoring of users' behavior has become increasingly sophisticated. Privacy-conscious consumers previously could usually delete or prevent the installation of cookie files through their Internet browser settings.[47] However, the tracking technology used "is getting smarter and more intrusive" with the use of "new tools that scan in real time what people are doing on a web page, then instantly assess location, income, shopping interests, and even medical conditions."[48] The study concluded, "One of the fastest growing businesses on the Internet is the business of spying on American consumers and tracking information."[49]

¶10 Because of such practices, there has been a push for the government to step in to regulate the Internet and promote greater consumer privacy.[50] However, while Congress is considering a federal online privacy law that would provide privacy protections for Internet users,[51] no consensus has yet been reached, and the online industry is warning that such a privacy bill could have negative effects on the already fragile U.S. economy by stifling the growth of the online advertising industry.[52]

¶11 Due to the lack of U.S. federal legislation in the field of privacy, some American Internet users have taken the issue to the courts. For instance, the U.S. District Court for the Northern District of California approved in March 2010 a $9.5 million settlement to a class action lawsuit challenging Facebook's Beacon program, an online advertisement system launched in late 2007 that monitored and published what users of the social networking site were buying on third-party sites such as Blockbuster.[53] The class action lawsuit claimed that users were not given adequate information about Beacon and that the

---

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *Id.*
[50] Declan McCullagh, *New Bill Renews Internet Privacy Fight*, CNET NEWS (July 20, 2010, 4:00 AM), http://news.cnet.com/8301-31921_3-20011016-281.html.
[51] Press Release, U.S. S. Comm. on Commerce, Sci., and Transp., *Consumer Online Privacy: Hearing Summary*, (Jul. 27, 2010), http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=4c76855f-f8b9-406f-a042-24f30741d58a.
[52] *See* Declan McCullagh, *Tech Firms Warn Privacy Bill Will Harm Economy*, CNET NEWS (July 23, 2010, 4:00 AM), http://news.cnet.com/8301-31921_3-20011435-281.html; McCullagh, *supra* note 50; Grant Gross, *Lawmakers Hear Mixed Reviews of Web Privacy Bill*, PC WORLD (July 22, 2010, 2:50 PM), http://www.pcworld.com/businesscenter/article/201712/lawmakers_hear_mixed_reviews_of_web_privacy_bill.html.
[53] Findings of Fact, Conclusions of Law, and Order Approving Settlement, *Lane v. Facebook, Inc.*, No. C 08-3845 RS, 2010 U.S. Dist. LEXIS 24762 (N.D. Cal. Mar. 17, 2010); *see also* David Kravets, *Judge Approves $9.5 Million Facebook 'Beacon' Accord*, WIRED (March 17, 2010), *available at* http://www.wired.com/threatlevel/2010/03/facebook-beacon-2/.

collection of personal information was done without their authorization or knowledge. Facebook has since shut down Beacon as part of the settlement. In addition, under the terms of the settlement, Facebook will contribute $9.5 million to set up a non-profit privacy foundation that will award grants to "projects and initiatives that promote the cause of online privacy, safety and security."[54]

¶12 In July 2010, a class action lawsuit was filed in the U.S. District Court in the Central District of California against online advertising firm Quantcast and a number of Internet giants such as MTV, ESPN, MySpace, Hulu, ABC, and NBC.[55] The plaintiffs allege that Quantcast created, on its partners' websites, cookies based on Adobe's Flash in order to track users across the Internet. The plaintiffs further allege that Quancast used such cookies to reconstruct browser cookies that users have previously deleted from their computers. This technique is often referred to as "re-spawning,"[56] and has already been condemned by Adobe.[57] The specific problem with Flash-based cookies is that, unlike traditional browser cookies, Flash cookies are not controlled through the user's browser controls for managing Internet privacy and most anti-tracking tools are not effective against Flash-based cookies. In addition, many Internet users are not aware of the existence of a distinction between cookies. According to a Quantcast representative, Quantcast has since fixed the issue and no longer restores deleted cookies.[58]

¶13 A similar class action lawsuit was filed in August 2010 in a California federal court alleging that one of Quantcast's rivals, Clearspring Technologies Inc., engaged in "a pattern of covert online surveillance" by providing its web widget "AddThis" to major websites.[59] This widget would install a tracking code on the computers of each user visiting those websites, and then track user behavior not only on partner websites, but

---

[54] The Ctr. for Democracy and Tech., Letter to Judge Seeborg (February 10, 2010), *available at* http://www.wired.com/images_blogs/threatlevel/2010/02/cdtfacebook.pdf (citing Settlement Agreement § 4.19, *Lane v. Facebook, Inc*., No. C 08-3845 RS, 2010 U.S. Dist. LEXIS 24762 (N.D. Cal. Mar. 17, 2010)); *see also* Findings of Fact, Conclusions of Law, and Order Approving Settlement, *supra* note 53; Kravets, *supra* note 53.

[55] Compl. at 4, *Edward Valdez v. Quancast Corp.*, No. CV10-5484 (C.D. Cal. July 23, 2010), http://online.wsj.com/public/resources/documents/cookielawsuit073010.pdf; *see also* Jennifer Valentino-DeVries, *Lawsuit Tackles Files That 'Re-Spawn' Tracking Cookies*, WALL ST. J. (July 30, 2010), *available at* http://blogs.wsj.com/digits/2010/07/30/lawsuit-tackles-files-that-re-spawn-tracking-cookies; Ryan Singel, *Privacy Lawsuit Targets Net Giants Over 'Zombie' Cookies*, WIRED (July 27, 2010), *available at* http://www.wired.com/threatlevel/2010/07/zombie-cookies-lawsuit/.

[56] Valentino-DeVries, *supra* note 55.

[57] Adobe Sys. Inc., *Comments from Adobe Sys. Inc.—Privacy Roundtables Project No. P095416*, at 2 (Jan. 27, 2010), http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf

> ("Adobe condemns the practice of using Local Storage to back up browser cookies for the purpose of restoring them later without user knowledge and express consent. This practice, also referred to as 'browser cookie re-spawning,' circumvents the user's intent to clear browser cookies and should not be used. . . . Adobe encourages users of the Adobe Flash Platform to use our technology responsibly and certainly not in ways that circumvents a user's privacy intentions.").

[58] *See* Ryan Singel, *Flash Cookie Researchers Spark Quantcast Change*, WIRED (Aug. 12, 2009), *available at* http://www.wired.com/epicenter/2009/08/flash-cookie-researchers-spark-quantcast-change/ ("QuantCast changed its code and updated its servers Tuesday afternoon after Wired.com published a story about the research, according to spokeswoman Christina Cubeta. . . . ' Quantcast no longer restores deleted cookies using values stored in Flash,' Cubeta said, describing the behavior as an 'unintended effect' of trying to have better web-traffic measurement.").

[59] Compl., *White v. Clearspring Techs. Inc.*, No. CV10-5948 (C.D. Cal. Aug.10, 2010), http://www.archive.org/download/gov.uscourts.cacd.479876/gov.uscourts.cacd.479876.1.1.pdf.

also beyond those websites.[60] The complaint also alleges that the tracking code has the ability to re-spawn cookies. The partner websites cited as defendants in the lawsuit include popular sites such as Disney, Playlist, Ustream, SodaHead, and Warner Brothers Records. Another similar lawsuit was filed in August 2010 against Specific Media,[61] the operator of one of the largest Internet advertising networks, also over its use of Flash to track users across the Internet and to recreate deleted cookies.[62]

¶14 To support their claims, plaintiffs in the *Quantcast*, *Clearspring*, and *Specific Media* cases relied on a study[63] performed by researchers at the University of California, Berkeley and other schools showing that an increasing amount of websites use Adobe's Flash to surreptitiously collect data on users.[64] The research found that fifty-four of the one hundred most popular sites use Flash cookies but that only four sites mention them in their privacy policies.[65] The study also outlined how Flash can be used to circumvent users' Internet settings since Flash is not affected by the browser controls for managing Internet privacy, and the study claimed that a significant amount of online advertising firms, including *Clearspring* and its rival *Quantcast*, use Flash cookies to restore traditional cookies after users had removed them.[66] The idea behind this tracking is to install two separate cookies on the user's machine—a traditional cookie that the user may erase through the browser's settings, and a Flash-based cookie that the user probably is not aware of.[67] It also found that this happened even for users who had expressly opted out of cookie tracking.[68]

---

[60] *See* Dean Takahashi, *Lawsuit Alleges Major Web Sites Spied on Users via AddThis Tool*, VENTURE BEAT (Aug. 14, 2010, 3:33 PM), http://venturebeat.com/2010/08/14/lawsuit-alleges-major-web-sites-spied-on-users-via-addthis-tool; Greg Sandoval, *Suit Alleges Disney, Other Top Sites Spied on Users*, CNET NEWS (Aug. 14, 2010, 3:33 PM), http://news.cnet.com/8301-31001_3-20013672-261.html.

[61] Compl., *La Court v. Specific Media Inc.*, No. CV10-01256 (C.D. Cal. Aug. 18, 2010), http://www.wired.com/images_blogs/epicenter/2010/08/No.-1-Attachement-1.pdf.

[62] *See* Ryan Singel, *Ad Firm Sued for Allegedly Re-Creating Deleted Cookies*, WIRED (Aug. 24, 2010), *available at* http://www.wired.com/epicenter/2010/08/specificmedia-zombie-cookie.

[63] Ashkan Soltani et al., *Flash Cookies and Privacy* (Aug. 10, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 ("We find that more than 50% of the sites in our sample are using Flash cookies to store information about the user. Some are using it to 'respawn' or re-instantiate HTTP cookies deleted by the user. Flash cookies often share the same values as HTTP cookies, and are even used on government websites to assign unique values to users. Privacy policies rarely disclose the presence of Flash cookies, and user controls for effectuating privacy preferences are lacking.").

[64] *Id.* at 2 ("We found that top 100 websites are using Flash cookies to 'respawn,' or recreate deleted HTTP cookies. This means that privacy-sensitive consumers who 'toss' their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies. Few websites disclose their use of Flash in privacy policies, and many companies using Flash are privacy certified by TRUSTe.").

[65] *Id.* at 2 ("We encountered Flash cookies on 54 of the top 100 sites. These 54 sites set a total of 157 Flash shared objects files yielding a total of 281 individual Flash cookies.").

[66] *Id.* at 3 ("For instance, a third-party ClearSpring Flash cookie respawned a matching Answers.com HTTP cookie. ClearSpring also respawned HTTP cookies served directly by Aol.com and Mapquest.com . . . . Upon deletion of cookies, the Flash cookie still allowed a respawn of the QuantCast HTML cookie.").

[67] *Local Shared Objects—"Flash Cookies"*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/cookies/flash.html (last visited Nov. 8, 2010).

[68] *Id.* at 3–4 ("The NAI (Network Advertising Initiative) is a cooperative of online marketing and analytics companies committed to building consumer awareness and establishing responsible business and data management practices and standards. Since some of the sites using Flash cookies also belong to the NAI, we tested the interaction of Flash cookies with the NAI opt-out cookie. We found that persistent

¶15 Such practices run afoul of European regulations since the European Union has enshrined the status of privacy as a fundamental right and has developed a comprehensive framework governing privacy since 1995. The EU Data Protection Directive (95/46/EC)[69] was implemented to standardize the requirements for the protection of personal information across all the countries within the EU. More recently, the European Union has enacted legislation that restricts the use of hidden identifiers to "trace the activities of the user" on electronic communication networks, such as cookies and similar tracking devices commonly used for online behavioral advertising.[70] The Directive on Privacy and Electronic Communications[71] (2002 ePrivacy Directive), which came into force on July 31, 2002, lays down the general legal principles applicable to the use of cookies. Thus, its preamble provides:

> However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.[72]

Article 5(3) of the 2002 ePrivacy Directive further provides:

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in

---

Flash cookies were still used when the NAI opt-out cookie for QuantCast was set. . . . Even when a user obtains a NAI opt-out cookie, Flash cookies are employed for unique user tracking. These experiences are not consonant with user expectations of private browsing and deleting cookies.").

[69] Council Directive 95/46, 1995 O.J. (L 281) 31–39 (EC) (Oct. 24, 1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[70] Council Directive 2002/58 (Directive on privacy and electronic communications), 2002 O.J. (L 201) 39 at (24) (EC) (July 12, 2002), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF.

[71] *Id.*

[72] 2002 O.J. (L201) 39, preamble at (25).

> accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user." [73]

Thus, the 2002 ePrivacy Directive acknowledged that devices such as cookies can be a legitimate tool, and subsequently, the user must have the possibility to refuse to have the cookie or similar device from being installed. The ePrivacy Directive also provides that the methods for providing the "clear and precise information," as required by the EU Data Protection Directive, and the right to refuse a cookie should be made as user-friendly as possible, but this information and choice can be provided at the initial connection to cover all subsequent uses.[74] In addition, access to specific website content may be made conditional on the acceptance of a cookie if it is used for a "legitimate purpose." Under the ePrivacy Directive, legitimate purposes include, "analysing the effectiveness of website design and advertising and verifying the identity of users engaged in on-line transactions"[75] (such as an online shopping cart for example), as well as "facilitating the transmission of a communication over an electronic communications network or where there is a need to provide an information service explicitly requested by the user."[76]

¶16 Equivalent laws are currently in place throughout the European Union since the Directive has been implemented in the national laws of the EU Member States. For instance, in the United Kingdom, the Privacy and Electronic Communications Regulations (Regulations)[77] is the national legislation implementing the 2002 ePrivacy Directive. Accordingly, § 6 of the Regulations provides that the Internet must not be used "to store information, or to gain access to information stored" on someone's computer, unless the user:

> (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
>
> (b) is given the opportunity to refuse the storage of or access to that information.[78]

However, the 2002 ePrivacy Directive is silent concerning how and when the opportunity to refuse the storage of, or access to the information, needs to be given, leaving each EU Member State (or more specifically, each country's court system) free to provide its own interpretation on these issues. For example, the United Kingdom's Information

---

[73] 2002 O.J. (L201) 44, art. 5 at (3).
[74] 2002 O.J. (L201) 39, preamble at (25).
[75] *Id.*
[76] 2002 O.J. (L201) 44, art. 5 at (3).
[77] The Privacy and Electronic Communications (EC Directive) Regulations, Sep. 18, 2003, No. 2426, *available at* http://www.legislation.gov.uk/uksi/2003/2426/contents/made.
[78] *Id.* § 6.

Commissioner has published guidelines concerning the use of cookies,[79] stating that "[a]t the very least, however, the user or subscriber should be given a clear choice as to whether or not they wish to allow a service provider to continue to store information on the terminal in question."[80] Since the user only needs to be given the choice whether or not to allow the service provider "to continue" to store information on the computer, this means that the cookie can already be present on the user's computer at the time when the choice is presented to the user. The Information Commissioner further adds:

> Where the relevant information is included in a privacy policy, for example, the policy should be clearly signposted at least on those pages where a user may enter a website. The relevant information should appear in the policy in a way that is suitably prominent and accessible and it should be worded so that all users and subscribers are able to easily understand and act upon it. [81]

As a result, under the 2002 ePrivacy Directive, it would seem acceptable to use cookies without obtaining the user's prior consent, provided that the use of the cookies is fully explained in a privacy policy which is accessible from every page of a site. The visitor only needs to be given a choice on whether or not he wishes the service provider to continue storing and accessing information on the user's computer. This is relatively easy to put in place, and most websites already comply with this guideline.

¶17 In order to strengthen the existing legal requirements concerning the "clear and comprehensive" information which must be given to the user, a new ePrivacy Directive[82] was enacted in November 2009 by the European Council, thereby amending the 2002 ePrivacy Directive. The 2009 ePrivacy Directive became effective in December 2009, however the amending Directive is not directly applicable and each EU Member State is required to modify its national law accordingly by June 18, 2011. The 2009 ePrivacy Directive provides in its recitals:

> Third parties may wish to store information on the equipment of a user, or gain access to information already stored, for a number of purposes, ranging from the legitimate (such as certain types of cookies) to those involving unwarranted intrusion into the private sphere (such as spyware or viruses). *It is therefore of paramount importance that users be provided with clear and comprehensive information when engaging in any activity which could result in such storage or gaining of access*. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user. Where it is technically possible and effective, in

---

[79] Information Commissioner's Office, *Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003*, (Nov. 30, 2006), *available at* http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/pecr_guidance_part2_1206.pdf.

[80] *Id.* at 5.

[81] *Id.*

[82] Council Directive 2009/136, 2009 O.J. (L 337) 11–36 (EC) (Nov. 25, 2009), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:EN:PDF.

> accordance with the relevant provisions of Directive 95/46/EC, *the user's consent to processing* may be expressed by using the appropriate settings of a browser or other application. The enforcement of these requirements should be made more effective by way of enhanced powers granted to the relevant national authorities.[83]

As in the 2002 ePrivacy Directive, the 2009 ePrivacy Directive stresses on the importance of providing users "with clear and comprehensive" information about the purposes of cookies or similar devices. However, under the 2009 ePrivacy Directive, the choice must be given whenever the user is "engaging in any activity which *could result* in such storage or gaining of access."[84] In other words, the choice must now be given *before* the service provider can begin storing and accessing information on the user's computer. The user's informed consent can only be *validly* obtained if prior information about the sending and purposes of the cookie has been given. This change is reflected in the amended Article 5(3) which now reads as follows:

> Member States shall ensure that the storing of information, *or the gaining of* access to information *already* stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned *has given his or her consent, having been* provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.[85]

Under the 2009 ePrivacy Directive, a cookie can be stored on a user's computer, or accessed from that computer, only after the user "has given his or her consent, *having been provided* with clear and comprehensive information."[86] As a result, the user of an Internet website will have to be notified of his or her privacy rights under a new *two-tiered* approach. The content provider will: (a) have to provide the user with clear and comprehensive information about the purposes of the processing (i.e., notice requirement), in accordance with the EU Data Protection Directive, *inter alia*, and then, (b) obtain the user's informed consent to the storage of or access to information on his or her computer (i.e., opt-in requirement), after having provided the required information requested under (a). The exceptions to the consent requirement are the same in both the 2002 and 2009 versions of the ePrivacy Directive.[87] It can be noted that whereas the 2002 ePrivacy Directive only referred to the user's "right to refuse," the 2009 ePrivacy Directive refers to both "the right to refuse" *and* the user's "consent" in both Article 5(3) and the recitals, probably to emphasize that the user must be presented with a clear choice and must be able to give "any freely given specific and informed indication of his

[83] 2009 O.J. (L 337) 20 at (66) (emphasis added).
[84] *Id.*
[85] 2009 O.J. (L 337) 30, at art. 2(5) (all addition in italics).
[86] *Id.*
[87] 2009 O.J. (L 337) 32, at art. 5(3).

wishes."[88] The change of language also implies that for the user's choice to be deemed valid under the 2009 ePrivacy Directive, consent must be freely given and constitute an informed indication of the user's wishes.

¶18 The application of the provisions in Article 5(3) does not require the "information" to be personal data within the definition of the EU Data Protection Directive, since Article 5(3) applies to all information stored or accessed.[89] However, if as a result of storing or accessing information through the cookie or other similar device, the information collected can be considered "personal data" then, in addition to Article 5(3) of the ePrivacy Directive, the EU Data Protection Directive will also apply.[90] In practice, almost all cookies involve the processing of personal data because even if the user's real identity remains anonymous, cookies typically involve the collection of the user's IP address, the processing of unique identifiers, or both which *are personal data* within the scope of the Data Protection Directive.[91] The fact that the user's real name or identity is not collected is irrelevant for purposes of the Data Protection Directive. Thus, the use of cookies or similar devices involving a unique user ID or an identifier will result in the application of both the Data Protection and the ePrivacy Directives. Cloud computing providers will therefore have to ensure compliance with both directives. Even though the 2009 ePrivacy Directive has yet to be incorporated into the national law of each EU Member State, it is very likely that the implementing legislation will closely follow the wording used in the 2009 Directive, since the EU Member States have already closely followed the language used in the 2002 ePrivacy Directive when enacting the implementing legislation.

¶19 Nevertheless, the question of how the user's consent may be obtained has been left unanswered by the 2009 ePrivacy Directive. The new ePrivacy Directive's recitals states, "The user's consent to processing may be expressed by using the appropriate settings of a browser or other application."[92] This means that when the user has set his or her browser settings to reject cookies, then such a privacy setting would be sufficient to indicate his or her refusal to allow the content provider to store information or to gain access to information stored on the computer. Subsequently, cookies may not be deployed on such a user's computer.

¶20 However, a problem arises if the user has kept the default privacy settings of his Internet browser. For instance, three major Internet browsers currently have as a default setting to allow all cookies, whereas only one major browser blocks third party cookies

---

[88] *See* Council Directive 95/46, supra note 69, at art. 2.

[89] Council Directive 95/46, 1995 O.J. (L 281), *supra* note 69, at art. 5(3).

[90] *See* Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising*, WP 171, at 9 (June 22, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

[91] *See* Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, WP148, at 9 (April 4, 2008), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf (In its *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, adopted on April 4, 2008, the EU Article 29 Working Party, an independent advisory body representing the European data protection and privacy authorities, confirmed that, in most cases, cookies and IP addresses are to be considered personal data. This Opinion stated: "When a cookie contains a unique user ID, this ID is clearly personal data. The use of persistent cookies or similar devices with a unique user ID allows tracking of users of a certain computer even when dynamic IP addresses are used. The behavioural data that is generated through the use of these devices allows focusing even more on the personal characteristics of the individual concerned.").

[92] Council Directive 2009/136, *supra* note 82, 20 at (66).

by default.[93] In such a situation, can informed consent be validly implied if the user has not changed the browser's default settings that are set to allow all cookies? And if a user chooses to install a browser that comes pre-installed with enhanced privacy settings to refuse cookies by default, should the user's refusal be implied from the browser's default settings?

¶21 To this end, the EU's *Article 29 Data Protection Working Party* (Working Party),[94] an independent advisory body representing the European data protection and privacy authorities, has issued an Opinion where it strongly objected to the idea of using the browser's default settings as a means to establish consent.[95] In the Opinion, the Working Party found that:

> [D]ata subjects cannot be deemed to have consented simply because they acquired/used a browser or other application which by default enables the collection and processing of their information. Average data subjects are not aware of the tracking of their online behaviour, the purposes of the tracking, etc. They are not always aware of how to use browser settings to reject cookies, even if this is included in privacy policies**.** *It is a fallacy to deem that on a general basis data subject inaction (he/she has not set the browser to refuse cookies) provides a clear and unambiguous indication of his/her wishes. . . .* [I]f the browser settings were predetermined to accept all cookies, such consent would not comply with Article 5(3) insofar as, in general, such consent cannot constitute a true indication of the data subject wishes. *Such consent would neither be specific nor prior (to the processing). Whereas a given data subject could indeed have decided to keep the settings to accept all 3rd party cookies, it would not be realistic for [content providers] to assume that the vast majority of data subjects who have their browsers "set" to accept cookies, effectively exercised this choice.*[96]

Browser settings may only deliver consent in very limited circumstances since the consent required needs to be specific, prior, and provide a clear and unambiguous indication of the user's wishes.[97] And since the user's consent needs to be freely given, it can also be revoked.[98] Consequently, a browser's default setting to refuse cookies will not necessarily have to be interpreted as a refusal by the user to have cookies installed, since the user can choose at any time to provide his consent and override the browser's

---

[93] Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising*, WP171 (June 22, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf.

[94] The Article 29 Data Protection Working Party was set up under Article 29 of the Data Protection Directive and is composed of representatives from the national data protection authorities of the EU Member States, the European Data Protection Supervisor and the European Commission. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[95] *See Opinion 2/2010 on Online Behavioural Advertising*, *supra* note 90, at 14.

[96] *Id.* (emphasis added).

[97] *Id.* at 17 (As noted by the Working Party, the problems related to obtaining informed consent are further emphasized as far as children are concerned. In addition to the requirements for consent to be deemed valid, "in some cases children's consent must be provided by their parents or other legal representatives.").

[98] *Id.* at 17 (stating that "*freely* given consent can always be revoked").

settings. The failure to comply with the adequate notice and consent requirements may give rise to liability, according to the Working Party:

> The Article 29 Working Party notes that the obligation to inform and other possible obligations may also derive from general principles of law (law of contracts and torts) as well as consumer protection laws related to business-to-consumer commercial practices such as Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').[99]

The Working Party did not go as far as to state that each website needs to ask each user to accept cookies at each connection. Instead, it said that advertising networks that provide advertisements to websites can simply obtain the user's consent, which would cover all the sites the network serves.[100] In addition, the user's acceptance of a cookie can be deemed to include not only the initial sending of the cookie, but also subsequent connections and collection of data arising from such a cookie.[101]

## III. SECURITY AND CONFIDENTIALITY OF INFORMATION IN THE CLOUD

¶22 In addition to these privacy issues, security in the cloud inherently raises even greater concerns than traditional desktop-based computing due to the intangible and "less visible" nature of the Internet. Because all the data is stored online instead of being stored on the user's desktop computer, the cloud could potentially pose huge security risks and put people's identities at risk. Thus, a survey carried out by Fortify Software amongst IT professionals at the DEF CON 2010 Hacker conference, has revealed that 96% of the respondents believed that hackers view the cloud as having "a silver lining."[102] Indeed, there is a strong belief that cloud providers are not doing enough to address the security issues in their services:

> 89% of respondents said they believed this was the case and, when you analyze this overwhelming response in the light of the fact that 45% of hackers said they had already tried to exploit vulnerabilities in the cloud, you begin to see the scale of the problem," said Barmak Meftah, chief products officer at Fortify. . . .

---

[99] *Id.* at 11 n.29.

[100] *Id.* at 16 ("In other words, the consent obtained to place the cookie and use the information to send targeting advertising would cover subsequent 'readings' of the cookie that take place every time the user visits a website partner of the ad network provider which initially placed the cookie.").

[101] *Id.* ("To avoid this problem, in accordance with Recital 25 of the ePrivacy Directive ('the right to refuse (cookies) may be offered once for the use of various devices to be installed on the user's terminal equipment . . . during subsequent connections'), users' acceptance of a cookie could be understood to be valid not only for the sending of the cookie but also for subsequent collection of data arising from such a cookie.").

[102] Press Release, Fortify Software, *DEF CON Survey Reveals Vast Scale of Cloud Hacking - and the Need to Bolster Security to Counter the Problem* (Aug. 24, 2010), https://www.fortify.com/news-and-events/press-releases/2010/2010-08-24.html.

> Remember, says Meftah, we are talking about hackers having DISCOVERED these types of vulnerabilities in the cloud, rather than merely making an observation.[103]

As a result, cloud vendors, and more generally the entire IT software industry will have to increase their security assurance strategies and governance. Nevertheless, a more pressing issue may be the emerging question of jurisdiction. In the world of the cloud, location is irrelevant since data simply flows around the globe. However, data that might be secure in one country may not be in another, and in many cases, users of cloud services do not know where their information is being held. To make matters worse, the existing legal structure is far from sufficient. In particular, data privacy laws vary from country to country, and the user's privacy will also vary significantly with the terms of service and privacy established by the cloud provider. Thus, a cloud computing platform would require users to create an account and establish their identity by filling out an online form and providing personal information (such as the user's name, home address, phone number, credit card number, etc.). This leaves a trail of personal information that, if not properly protected, may be exploited and abused. For instance, the World Privacy Forum released a report on cloud computing, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*,[104] where it recognized the significant implications for the confidentiality of personal, business, and governmental information, and highlighted privacy concerns due to the relatively new nature of cloud computing:

> Legal uncertainties make it difficult to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users. The law badly trails technology, and the application of old law to new technology can be unpredictable. For example, current laws that protect electronic communications may or may not apply to cloud computing communications or they may apply differently to different aspects of cloud computing.[105]

With the growing adoption of cloud computing, there will undoubtedly be a significant increase in the amount of commercial, personal, and even secret data and other sensitive information (such as business plans or research and development) flowing around the globe in the cloud. However, users will also expect the cloud provider to ensure the confidentiality of their information and to prevent any unauthorized access.

¶23 Because of this legal uncertainty, a broad array of technology companies, civil rights organizations, think tanks, advocates from across the political spectrum, lawyers, and academics have banded together to launch the Digital Due Process (DDP).[106] The DDP is a coalition focused on helping modernize current legislation governing how law

---

[103] *Id*.

[104] *See* Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, WORLD PRIVACY FORUM (FEB. 23, 2009), *available at* http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[105] *Id.* at 7.

[106] *See* Press Release, Digital Due Process, *Advocacy Groups, Companies Call for an Update of the Privacy Framework for Law Enforcement Access to Digital Information Broad Coalition Seeks to Balance Law Enforcement Needs, Privacy, and Innovation* (Mar. 30, 2010), http://www.digitaldueprocess.org/index.cfm?objectid=3EFF6654-383D-11DF-84C7000C296BA163.

enforcement agencies may gain access to electronic data.[107] In particular, the coalition is seeking a reform of the U.S. Electronic Communications Privacy Act of 1986[108] (ECPA), calling for it to be updated to account for recent and emerging technologies, including email, social networking, and cloud computing.[109] For instance, under current U.S. law, the privacy rights concerning an e-mail or an electronic file differs depending on whether it is stored on the user's hard drive or "in the cloud."[110] More than twenty organizations have joined the Digital Due Process coalition, including AT&T, Google, Microsoft, Intel, AOL, eBay, Amazon, Salesforce.com, Loopt, the Center for Democracy & Technology, the American Civil Liberties Union, the Electronic Frontier Foundation, and Americans for Tax Reform. Microsoft is also pushing for a Cloud Computing Advancement Act to enhance privacy and security protections and foster the development of the cloud.[111] The Electronic Privacy Information Center (EPIC), an electronic privacy advocacy group, already submitted a complaint to the FTC against Google, and concerning cloud computing security and privacy generally.[112]

¶24 Outside of the United States, an often mentioned hurdle to the international adoption of cloud computing is the USA Patriot Act of 2001,[113] which expands law enforcement's surveillance and investigative powers and grants the U.S. government a right to demand data on the grounds of homeland security. Such concerns are hindering the adoption of cloud-based solutions outside of the United States through fear that innocent but sensitive information might become snared in a U.S. investigation,[114] even

---

[107] *Id.*

[108] Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, Oct. 21, 1986, 100 Stat. 1848, (codified at 18 U.S.C. § 2510 (2006)).

[109] *See* Miguel Helft, *Technology Coalition Seeks Stronger Privacy Laws*, N.Y. TIMES, Mar. 31, 2010, at B1; Digital Due Process, *About the Issue*, http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Nov. 8, 2010).

[110] *See* J. Beckwith Burr, *The Electronic Communications Privacy Act of 1986: Principles for Reform* (March 30, 2010), at 5–12, http://digitaldueprocess.org/files/DDP_Burr_Memo.pdf ("The privacy rights of an individual with respect to all of this information, if stored on his or her hard-drive—or indeed on a CD in a safe deposit box—would be fully protected by the warrant clause. Under ECPA, however, a single email or electronic document could be subject to multiple legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient or uploaded into a user's 'vault' in the cloud, where it might be subject to an entirely different standard. . . . The different standards are the unanticipated by-product of technology changes, and not a careful balancing of the needs of law enforcement and the privacy rights of individuals. Nor do they reflect a substantive difference in the nature of the information; rather they reflect the fact that ECPA was enacted in 1986—six years before Congress authorized commercial activity on the Internet, and seven years before the first web browser was introduced.").

[111] *See* Brad Smith, General Counsel, Microsoft, *Building Confidence in the Cloud: The Need for Prompt Industry and Government Action for Cloud Computing*, Presentation at the Brookings Institution Policy Forum on "Cloud Computing for Business and Society", at 1 (Jan. 20, 2010), *available at* http://blog.seattlepi.com/microsoft/library/20100120smithspeech.pdf ("The world needs a safe and open cloud—a cloud that is protected from the efforts of thieves and hackers and also that serves as an open source of information to all people around the world. Neither goal may be fully achieved today—but we have to keep striving to achieve them over time. These issues are important in countries around the world.").

[112] *See* Cecilia Kang , *Privacy Advocates File FTC Complaint on Google Buzz*, WASH. POST (Feb. 17 2010), *available at* http://voices.washingtonpost.com/posttech/2010/02/privacy_advocates_file_complai.html.

[113] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter Patriot Act] (codified in scattered titles of U.S.C.).

[114] *See, e.g.*, Michael Vizard, *Patriot Act May Hamper Cloud Computing Adoption*, IT BUSINESS EDGE

though similar legislation already exists in other countries.[115] For instance, according Informatica, a major provider of enterprise data integration software:

> [T]he USA PATRIOT act is a definite no-go for many European customers. They simply cannot accept that the US government could potentially look at data streams into their financial applications. Taking into account both of these obstacles, a European back-office manager will probably not even listen to an American vendor offering a cloud computing integration service."[116]

Within the European Union, the main concern for businesses is not so much the potential impact of the USA Patriot Act, but rather whether the storage of customer data outside of the European Union would be a violation of the EU's Data Protection Directive[117] and therefore, of the EU Member State's national law implementing the EU Data Protection Directive. The Data Protection Directive sets the applicable legal framework with regard to the protection of individuals' confidential data and prohibits organizations from passing on that data without the customer's prior consent. It focuses primarily on the "processing" of "personal data," which is defined as any information relating to an identified or identifiable "data subject," or natural person.[118] "Processing" covers almost any operation involving personal data, including the collection, review, use, disclosure of personal data to any third party, disposal, and virtually any other action with personal data.[119] Accordingly, uploading data into the cloud is considered "processing" under the Data Protection Directive. In addition, the Directive applies to both public and private organizations and those that, although not established in the EU, use equipment located there to process personal data.[120] Accordingly, whenever a cloud computing company sets up a data center or servers within the EU, it becomes subject to the Data Protection Directive. It should be noted that the EU Member States' courts interpret the term "equipment" broadly. For instance, the use of a hosting server will lead to the application of the Data Protection Directive; however, the mere use of a personal computer or even browser cookies has also been considered to be "processing" within the scope of the Data Protection Directive.[121] The fact that the user's real name or identity is not collected is irrelevant for purposes of the Data Protection Directive; as long as a unique user ID or an identifier is involved, the Data Protection Directive is applicable.

---

(Dec. 29, 2009, 9:30 AM), http://www.itbusinessedge.com/cm/blogs/vizard/patriot-act-may-hamper-cloud-computing-adoption/?cs=38395; Brian Jackson, *Canadian Firms Shy from Cloud Because of Patriot Act*, ITBUSINESS.CA (May 20, 2010, 5:00 AM), http://www.itbusiness.ca/it/client/en/home/News.asp?id=57655.

[115] *See*, Jennifer Kavur, *Don't Use the Patriot Act as an Excuse*, ITWORLD CANADA (Jul. 5, 2010), http://www.itworldcanada.com/news/dont-use-the-patriot-act-as-an-excuse/141033.

[116] Stefan Ried, *Informatica's Cloud Service Is Flying Under The Radar Especially For European Customers*, FORRESTER (July 6, 2010), http://blogs.forrester.com/stefan_ried/10-07-06-informaticas_cloud_service_flying_under_radar_especially_european_customers.

[117] *See* Council Directive 95/46, *supra* note 69.

[118] *Id.*

[119] Council Directive 95/46, 1995 O.J. (L 281), *supra* note 69, at art. 2.

[120] *Id.*

[121] *See Opinion 1/2008 on Data Protection Issues Related to Search Engines*, *supra* note 91; *see also* Sophie Louveaux, *Le Commerce Électronique et la vie Privée* (*Electronic Commerce and Private Life*), LE DROIT DES AFFAIRES EN ÉVOLUTION - LE COMMERCE ÉLECTRONIQUE (BUSINESS LAW IN EVOLUTION – ELECTRONIC COMMERCE), Bruylant-Kluwer (2000).

¶25 The Data Protection Directive sets forth a number of obligations applicable to "data controllers and processors." With regard to cloud computing specifically, the characterization of an entity as either a "controller" or a "processor" under the Data Protection Directive will depend on the type of cloud computing system used.[122] A controller is defined in Article 2 as the natural or legal person or public agency that "alone or jointly with others" determines "the purposes and means of processing" personal data.[123] A processor is a natural or legal person or agency that processes data on behalf of a controller.[124] There are, however, obligations imposed which are common to both categories. Thus, cloud providers have security requirements and must "implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access."[125] Accordingly, authentication and access safeguards must be robust and ensure an "appropriate" level of security.

¶26 In addition, the processing of personal data must be fair, adequate, relevant, for legitimate purposes, and not excessive in relation to the purpose for which it was collected.[126] The personal data must be processed for purposes compatible with those for which it was initially collected.[127] Whether personal data are obtained directly from an individual or from other sources, individuals must consent to the collection of the data and be told who is collecting the data, why it is being collected and "any further information" required to make the processing "fair" to the individual.[128] The additional information may include, for instance, who will receive the data, rights of access to the data (in particular, to block, rectify, or delete such data), and whether the data is legally required or not.[129] Subsequently, this information, and in particular the individual's rights of access to the data, should be addressed in the service provider's agreement in order to avoid further difficulties.

¶27 The most notable requirement of the Data Protection Directive is that it places restrictions on the transfer of personal data outside of the European Union. Such data may only be transferred outside of the EU if that country provides an "adequate" level of protection; otherwise specific compliance measures are required for such a transfer to take place.[130] Only a small handful of countries, such as Argentina, Canada, and Switzerland, are deemed to have an "adequate" level of data protection under the Data Protection Directive.[131] Most notably, the United States is not among the countries deemed to have an adequate level of protection.[132] In addition, countries such as China,

---

[122] *See* Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*, WP169 (Feb. 16, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[123] *See* Council Directive 95/46, *supra* note 69, at art. 2.

[124] *Id.*

[125] *Id.* at art. 17.

[126] *Id.* at art. 6.

[127] *Id.*

[128] *Id.* at art. 11.

[129] *Id.* at art. 12.

[130] *Id.* at art. 25–26.

[131] *See Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (last visited Nov. 8, 2010).

[132] *Id.*

India, the Philippines, South Africa, and other common locations for outsourcing are not deemed to provide an adequate level of protection under the EU Data Protection Directive.[133] As a result, cloud computing could run afoul of EU rules unless specific measures are taken to comply with the EU Data Protection Directive.

¶28 The most simple and obvious way to comply with the EU Data Protection Directive is to ensure that personal data does not leave the EU and to have the cloud computing service provided within the EU, which is why certain cloud vendors offer segregated EU clouds that keep personal data from being transferred outside of the European Union. However, such a segregation is not always possible due to the nature of cloud computing. One could envision cloud services obtaining the informed consent of each individual to permit the transfer of his or her personal data outside of the EU in order to comply with the Data Protection Directive, although such solution is not practicable on a large scale.

¶29 In order to permit the transfer of personal data from the EU to the United States while assuring an "adequate" privacy protection overseas, the International Safe Harbor Certification[134] program was developed by the U.S. Department of Commerce. Under this program, U.S. companies can publicly certify compliance with a standard set of Safe Harbor Privacy Principles approved by the European Commission, in order to ensure an "adequate level of protection" of the personal data, as required by the Data Protection Directive. However, should the data be stored on servers located outside of both the EU and the United States, the Safe Harbor Program is ineffective.

¶30 In order to enable the transfer of data from the EU to non-EU countries while assuring privacy protection overseas and compliance with the Data Protection Directive, contractual clauses can be used to enable the transfer of personal information. To this end, the European Commission has devised a set of EU-approved standard contract clauses or "Model Contracts,"[135] which were recently updated to better address the trend toward outsourcing and sub-processing (including cloud computing).[136] Finally, a multinational group of corporations may transfer personal data outside of the European Union, but still within the group, if it can ensure an "adequate level of protection" of the personal data. This adequacy can be achieved by the adoption of binding rules of corporate conduct by the group, also known as "Binding Corporate Rules."[137] Nevertheless, it should be noted that such Model Contracts or Binding Corporate Rules alone may not necessarily be sufficient regarding cloud provider relationships because, under the EU Data Protection Directive, all parties handling the data need to be subject to the *same obligations* of confidentiality and security. None of these issues are insurmountable, but they will require a careful analysis from multinational corporations before they can jump into the cloud.

---

[133] *Id.*

[134] *Safe Harbor Overview*, http://www.export.gov/safeharbor/eg_main_018236.asp (last updated Jan. 14, 2010, 3:56 PM).

[135] *See Model Contracts for the Transfer of Personal Data to Third Countries*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm (last visited Nov. 8, 2010).

[136] *See Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC of the European Parliament and of the Council* (Feb. 5, 2010), EUROPEAN COMMISSION, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

[137] *Glossary: Binding Corporate Rules*, European Data Protection Supervisor, http://www.edps.europa.eu/EDPSWEB/edps/Home/EDPS/Dataprotection/Glossary/pid/72 (last visited Nov. 8, 2010).

## IV. CONCLUSION

¶31 As cloud computing becomes more widely used by individuals and businesses alike and is increasingly viewed as a cheap, convenient, and viable alternative to the traditional desktop computer platform, the law is unfortunately still trailing behind the development of new technology. There is a great deal of uncertainty in how laws enacted in the mid-80s, such as the ECPA, will apply to cloud computing. A growing number of customers are becoming mindful of their privacy online and are worried about their sensitive and confidential data stored in the cloud. Since it is expected that more and more sensitive data will be stored in the cloud, there is a real need for the law to be updated around the issues of data security and privacy in order to accommodate today's realities. The issue is similar within the European Union where there is still some uncertainty regarding the extent of the rules within a cloud computing environment. A reform proposal to the EU Data Protection Directive is expected in the latter half of 2011, according to the French Data Protection Authority (CNIL).[138]

¶32 Meanwhile, it is very important for corporations to comply with existing EU regulations and take into account privacy when designing cloud services, particularly whenever there is a collection, processing, or sharing of personal data. Cloud providers must ensure that the personal data collected is fair, adequate, relevant, and not excessive in relation to the purpose for which it was collected. The personal data processed must be compatible with the purpose for which it was initially collected. More importantly, the cloud provider must ensure an "appropriate" level of security. As a result, the importance of data privacy as a major component of corporate compliance has become undeniable—and it can safely be assumed that this trend will continue in the next few years.

[138] *La Révision de la Directive Européenne ne doit pas se aire dans la Précipitation* (*The Revision of the European Directive Must not Be Done in a Hurry*), CNIL (Aug. 2, 2010), http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-revision-de-la-directive-europeenne-ne-doit-pas-se-faire-dans-la-precipitation/.