

JANUARY 2011

PROTECTING CONSUMERS AND PROMOTING INNOVATION AND GROWTH IN CLOUD COMPUTING

Executive Summary

It has become increasingly clear that we are on the cusp of a seismic shift in technology. Driven by innovations in cloud computing, we are poised once again to transform our relationship with computers, just as we did during the transition from massive mainframes to desktop PCs in the 1980s. Ubiquity will be the name of this new game. Consumers will use increasingly smaller yet more powerful handheld devices to access information and content in the cloud from wherever, whenever. And *any* user with a high-speed Internet connection – from a health clinic in a remote village to an Internet start-up in a dense urban center – will have affordable access to a level of computing power that until recently was available only to entities with large IT budgets and in-house expertise.

Properly deployed, the cloud promises not only to redefine our relationship to computing, but also to spur investment and create new jobs – opportunities that are much needed during this time of sluggish economic growth. In Europe, for example, cloud computing could create an estimated one million new jobs and several hundred thousand new small- and medium-sized enterprises (SMEs).¹ In the U.S., cloud services could add more than \$166 billion in new business revenues by 2013.² And the Asia/Pacific region, where over half of SMEs surveyed already see the cloud as a tool to grow their businesses,³ will benefit from the cloud too.

The pieces necessary to launch this transformation are falling into place. Across the globe, there are now nearly two billion Internet users – an increase of 450% over the last decade.⁴ In parallel, more and more people around the world are gaining access to the cloud through high-speed broadband connections. Mobile wireless growth, in particular, has exceeded expectations, and by 2014 mobile data traffic is expected to be *39 times* greater than the levels seen in 2009.⁵ To harness these potential opportunities, policymakers in Europe have adopted a sweeping “Digital Agenda” – a series of ambitious measures that includes investments in broadband infrastructure and skills training alongside a host of reforms aimed at ensuring existing regulatory frameworks are suited to current realities.⁶ The U.S. is taking similar steps to promote innovation through its National Broadband Plan, which among

¹ F. Etro, *The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe*, Review of Business and Economics, 2009/2, pp. 191, 192. For more information on this study, see <http://www.voxeu.org/index.php?q=node/4671>.

² See Microsoft on the Issues, *IT Employment and Innovation Fostering Recovery* (September 30, 2010) (reporting on economic study by research firm IDC), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/09/30/it-employment-and-innovation-fostering-recovery.aspx.

³ See Press Release, *IDC Says Cloud Computing is More than Just Hype; Worldwide IT Spending on Cloud Services Expected to Reach US \$42 Billion by 2012* (March 6, 2009), <http://www.idc.com/AP/pressrelease.jsp?containerId=prSG21724009>.

⁴ Statistics on world Internet usage are available at <http://www.internetworldstats.com/stats4.htm>.

⁵ See Cisco Systems, *Cisco Visual Networking Index Global Mobile Data Forecast 2009-2014* (February 9, 2010), http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

⁶ Communication on A Digital Agenda for Europe COM(2010) 245 final/2, [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245\(01\):EN:NOT](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245(01):EN:NOT).

other initiatives sets a goal of providing at least 100 million U.S. households with affordable broadband connections at download speeds of 100 Mbps and upload speeds of 50 Mbps by 2020.⁷

These are promising developments. But we must work harder to ensure that cloud users have confidence that as their data moves from the desktop to the cloud, it will stay private and secure, and that regulatory regimes are fit for an era in which information may be created in France using software hosted in Poland, stored in Canada, backed up in a data centre in Singapore, accessed by support personnel in India, and then accessed again for business purposes by the creators in France. This White Paper seeks to contribute to the dialogue on the steps necessary to move us closer towards that goal.

I. Consumers and businesses are excited about the potential of the cloud, but they continue to have concerns about the privacy and security of their data.

Cloud computing has been around for some time – consider, for example, web-based personal email accounts – but it has primarily been used by consumers. Today, a combination of sophisticated software, pervasive and interconnected devices, and ever-faster broadband connections is allowing governments and businesses to move beyond in-house IT systems to a more flexible model based on applications and services delivered over the Internet. These public and private sector users enjoy a range of benefits, including:

- *Cost savings.* Because the cloud frees users of the need to maintain their own IT infrastructure, they are able to spend their IT budgets more effectively and devote more of their human capital resources to their core business functions. Savings will increase as clouds grow: economists estimate that the combined impact of consolidating overhead and power costs and pooling computing resources can result in long-term savings of up to 80% when comparing large and small clouds.⁸
- *New opportunities for all.* With cloud computing, organizations of any size and in virtually any location can tap into supercomputing power and software applications that previously were available only to the largest global companies. People also can build entirely new computing tools in the cloud.
- *Increased agility and speed.* Unprecedented computing power and storage capacity now available in the cloud allows organizations to roll out new applications and services with significantly greater speed – and less risk – than in the past. Services that once would have required large capital investments and lengthy deployments can be launched in a matter of weeks or even days.
- *Reduced carbon footprint.* Studies show that the cloud can produce real energy-efficiencies and reduce the carbon footprint of many business applications, thereby helping governments and

⁷ See *Connecting America: The National Broadband Plan*, § 2 (March 16, 2010), <http://www.broadband.gov/plan/2-goals-for-a-high-performance-america/>.

⁸ See Microsoft, *The Economics of Cloud Computing for the EU Public Sector*, <http://www.microsoft.eu/Cloudeconomics.aspx>.

industry achieve their green goals, reduce the environmental impact of IT, and enable a greener society.⁹

In light of these benefits, it is not surprising that users are enthusiastic about the cloud. For example, KPMG in the Netherlands found last year that an overwhelming 59 percent of Dutch decision-makers and business leaders agree that “cloud computing is the future model of IT.”¹⁰ Enthusiasm for the cloud is high in the U.S. as well. A survey conducted by Penn Schoen Berland for Microsoft found that 58 percent of consumers and 86 percent of senior business leaders in the U.S. are excited about the potential of cloud computing to change the way they use technology.¹¹ The majority of consumers and business leaders believe these technologies can help government operate more efficiently and effectively as well.

That’s the good news. The less good news is that almost every survey on the cloud also reveals that users are concerned about privacy and security. For example, a 2010 survey by the World Economic Forum found that 90 percent of respondents in Europe see privacy as a “very serious” constraint on adopting cloud computing.¹² As people and organizations around the world move information from desktops to their mobile devices and into the cloud, they want to know that their data will remain safe and protected.

In Europe, Digital Agenda Commissioner Neelie Kroes has taken up this issue and urged the adoption of “clear and cloud-friendly rules . . . [because] a ‘cloud’ without clear and strong data protection is not the sort of cloud we need.” Likewise, the U.S. Department of Commerce recently observed that the ability to “safely use services such as cloud-based email and file storage to their full potential depends on privacy protections that are consistent with other computing models.”¹³ We agree. Put simply, it is in the collective interest of all stakeholders that cloud users have well-founded confidence in the cloud.

Addressing privacy and security concerns in the cloud is industry’s responsibility in the first instance. Microsoft fully embraces this responsibility, and the next section describes some of the many ways in which we are engaging with our customers to help them understand their rights and make informed choices when using cloud computing. Governments also have a critical role to play and the remaining sections of the paper propose steps that they can take to promote privacy and security in cloud computing, including updating legal frameworks to make clear whose laws apply – and how they apply – to data in the cloud and avoiding overly restrictive laws on the movement of data across

⁹ *Id.* and Microsoft, *Cloud Computing and Sustainability* report, <http://www.microsoft.com/environment/cloud>.

¹⁰ KPMG, *From Hype to Future: KPMG’s Cloud Computing Survey* (2010), http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Documents/PDF/IT%20Performance/From_Hype_to_Future.pdf.

¹¹ See Penn Schoen Berland, *Cloud Computing Flash Poll* (2009), www.microsoft.com/presspass/presskits/cloudpolicy/docs/CCTopline.ppt.

¹² World Economic Forum, *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation* (2010), http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf.

¹³ See The Department of Commerce Internet Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (December 2010) <http://www.commerce.gov/sites/default/files/documents/2010/december/ijtf-privacy-green-paper.pdf>.

borders. A proactive but balanced approach will best help spur innovation and drive resulting investment, job opportunities, and other benefits.

II. Industry must listen and respond to user concerns, both by providing innovative solutions that protect data and by adopting and adhering to appropriate, common codes of conduct. As a company, we are committed to doing our part.

As with all businesses, cloud service providers who want to be competitive must listen and respond to their customers. Microsoft is committed to playing a proactive and responsible role in this area. We firmly believe that privacy practices in the cloud will benefit from an ongoing dialogue with customers, both directly with enterprise customers and more broadly with consumers through communications and services that inform consumers and compare offerings. By way of analogy, in the automotive industry, this sort of dialogue has been successful at driving industry to innovate in the area of safety – through government initiatives to inform consumers as well as consumer magazines and websites that rate cars based in part on safety standards and consumer input. A similar dialogue in the cloud computing context could facilitate industry responsiveness to consumer privacy needs.

Microsoft, for its part, obtains customer feedback through a variety of means, including usability tests, surveys, focus groups and other types of field research. Our help features, for example, ask users to assess the quality of our responses to frequently asked questions – enabling us to better ensure that the information we’re providing is clear, cogent and otherwise meets the needs of our customers. We also created the Customer Experience Improvement Program (CEIP), through which consumers may voluntarily share information online about how they use Microsoft programs and report any problems they may encounter. This information helps us to innovate and improve the overall user experience, including with respect to privacy and security.

What we have learned from this feedback, among other things, is that consumers want to better understand what data is being collected and how it is being used. In response, we have worked hard to provide clear and easy-to-understand information on our privacy and security practices. For example, Microsoft was among the first companies to introduce a layered privacy notice for its online services – providing consumers with a clear, concise one-page summary of the company’s privacy practices with links to full statements and other relevant information.¹⁴ We also were one of the first software manufacturers to provide layered notices in relation to our software products. (For enterprise customers, we recognized the need to address the two-tiered nature of protecting our enterprise customers’ privacy, and therefore we use the same convention that we employ for consumer privacy notices,¹⁵ and also help our enterprise customers with their responsibilities regarding their consumers’ and partners’ privacy.¹⁶)

¹⁴ The layered notice for Microsoft’s online services can be found at <http://privacy.microsoft.com/en-us/default.mspx>.

¹⁵ The layered notice for Microsoft’s enterprise-focused online services can be found at <http://www.microsoft.com/online/legal/?langid=en-us>.

¹⁶ For example, we have provided the following clear guidance in our agreements to our enterprise customers regarding the use of their enterprise data: “Customer data will be used only to provide you the online service. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the online service and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam).”

On top of transparency, it is clear that consumers also want choice and control over *how* their data is used – particularly by third parties. Again, we are working hard to be responsive. The upcoming version of our browser, Internet Explorer 9 (IE9), will provide an innovative new feature, “Tracking Protection.” On today’s Internet, websites increasingly pull in content, such as images and text, from third party sites. Although this is a common feature of modern web design that enables online providers to enhance their websites and services, users sometimes are not aware that they can be tracked across the web by third parties through content on the pages. Tracking Protection filters out content on a page that may have an impact on user privacy. Specifically, users will be able to create Tracking Protection Lists that allow users to limit the sharing of their data with specified sites, or categories of sites. Users may include whatever sites they desire in these lists, and in the future we expect people will be able to choose Tracking Protection Lists that are created by all kinds of companies and organizations – from privacy advocates to security firms to advertising trade groups. Importantly, Tracking Protection puts users in control without employing intrusive mechanisms that detract from the online experience, such as interrupting users potentially hundreds of times a day to request affirmative consent every time a cookie is deployed.¹⁷ The European Privacy Association recently praised Tracking Protection as contributing to “the creation of an online market more focused on consumers’ needs and attentive to their privacy concerns.”¹⁸

Microsoft gives consumers similar levels of choice and control across our technologies and services. Windows Phone 7, for instance, includes a geolocation feature that enables customers to take advantage of the increasing array of location-based applications and services on the market. However, no application can gain access to that location information unless the customer has provided affirmative consent. Applications that use a customer’s location also are required to allow users to turn off that access at a later time – and customers have the option of turning off location access for all applications.

We also provide our enterprise customers with sophisticated tools for managing the use of sensitive information within their own organizations – using innovations such as Windows 7 BitLocker and BitLocker To Go, which encrypt data on PCs and portable USB devices and thereby prevent access to an organization’s sensitive data if an employee device is lost or stolen.¹⁹

Ultimately, these efforts towards transparency and user control come together in our approach to “Privacy by Design.” For us, Privacy by Design means that we engineer privacy into our products and online services at the outset of development; review all products and services to identify privacy issues at an early stage; help product groups follow Microsoft privacy policies and standards; and encourage the continued consideration of privacy and data security throughout the project lifecycle, including following the release of the product or service onto the market. This methodical approach to

¹⁷ More information on our Tracking Protection feature is available at <http://bit.ly/ietpl>. While Tracking Protection is a new feature, it builds on protections in our current browser, IE8. With IE8, we introduced InPrivate Filtering, which when enabled by users blocks third-party content that appears with a high frequency across sites visited (because of the volume of information they receive, high-frequency sites have the greatest ability to build a profile of the user over time).

¹⁸ European Privacy Association, *Protection list: on the Right Track*, January 21, 2011, http://www.europeanprivacyassociation.eu/2009/agenda_news.asp?funzione=scheda&id=36

¹⁹ For more information on security tools provided in Windows 7, see <http://www.microsoft.com/windows/enterprise/business-priorities/security.aspx>. In addition, Microsoft certifies its online services to the ISO 27000 series of security standards, which among other things establish guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

privacy builds on our long history of enhancing privacy protections to evolve with customer needs and legal frameworks.

In short, Microsoft is committed to maintaining leadership in the industry on privacy in the cloud. Why? In addition to our firmly held convictions about privacy and security, our business model – which is built on generating revenue from the sale of innovative software and services – drives us to protect user privacy. In contrast, other companies generate revenue almost exclusively by monetizing consumers' personal data for advertising. This leads to very different incentives and approaches on privacy and protecting consumers. Because of our business model, we view privacy as having tremendous commercial value to users, and we believe that Microsoft and others in industry should compete to provide the best privacy protections available.

Of course, while competition will produce many benefits in the privacy arena, industry collaboration and self-regulation are also critical to promote online privacy – a point that the European Commission recognizes in its Digital Agenda for Europe.²⁰ That is why Microsoft shares with partners and competitors the privacy guidelines we follow when developing software and online services.²¹ Since we first made these guidelines available in 2006, they have made significant contributions to the leading professional privacy certification in the IT sector (the Certified Information Privacy Professional for IT, or CIPP/IT) and have helped to shape international privacy standards.

We have also participated actively in a number of other cross-industry collaborations. One example is the Safer Social Networking Principles in the EU, which is the result of a 2008 initiative by the European Commission that brought together 20 providers of social networking and related services to address concerns about the safety of children in the social networking environment. These providers worked openly and collaboratively to develop rules and principles of child online safety to which they voluntarily committed to adhere. Another example is the Self-Regulatory Program for Online Behavioral Advertising. In that recently launched initiative, the largest media and marketing associations in the U.S., along with the Better Business Bureau and the Network Advertising Initiative (NAI), launched a program to provide consumers with a better understanding of, and greater control over, advertisements that are personalized based on their online activities. The Self-Regulatory Program encourages companies that engage in online behavioral advertising to display an icon prominently in or near behaviorally targeted ads. By clicking on the icon, consumers can easily learn about online behavioral advertising and the privacy practices associated with the particular advertisements they receive, and they can opt out of behavioral advertising if they choose.

We see a number of opportunities for further dialogue with industry partners on self-regulation. For example, as geolocation data is increasingly being collected and used to provide a range of services to users, several organizations are leading efforts to create codes of conduct to help assuage emerging concerns of regulators around the collection and use of such data. Microsoft will continue to actively participate in and support efforts to help create coherent, privacy protecting practices across the industry.

²⁰ See Section 2.3 (Trust and Security) of the Communication on *A Digital Agenda for Europe*, *supra* note 6.

²¹ The guidelines are available at <http://go.microsoft.com/?linkid=9746120>.

III. Governments should take steps to ensure that existing regulatory frameworks are suited to the cloud.

Given the economic and social benefits of cloud computing, governments have a compelling interest in nurturing the adoption of cloud services. A robust, safe, and secure cloud requires governments to take a balanced approach that sets out clearly-defined guidelines for cloud vendors to maintain high levels of data protection but at the same time does not preclude industry innovation in new ways of providing those protections.

Governments in a number of markets have taken or are now taking initiatives that exemplify the benefits of balanced approaches to reform. Consider, for example, Article 17 of the EU Data Protection Directive, which requires data controllers to deploy security measures to protect data. Rather than dictating and freezing in time the precise type of measures to be employed, Article 17 simply demands that security measures achieve a level of security appropriate to the risks associated with the processing and nature of the data in question. This flexibility allows industry to develop new means to secure data, often in response to rapidly evolving security threats, as long as those means actually achieve an appropriate level of security.

Similarly, the U.S. Federal Trade Commission's (FTC) proposed privacy framework encourages online providers to develop and implement comprehensive privacy programs for training employees and promoting accountability, but recognizes that these programs should be tailored so that they are "appropriate to the risks presented to the data." Rather than imposing a rigid prescriptive rule, the FTC emphasized a context-based approach in which "companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data or data of a sensitive nature."²² Microsoft supports this and other proposals that set a baseline protection for data privacy and security while allowing industry to build on that baseline in a pragmatic, meaningful, and effective way.

At the same time, in many cases current legal frameworks impose inflexible mandates that do not allow consideration of the contexts in which consumer data is collected and used. Indeed, even in the case of Article 17, many EU Member States implemented it in conjunction with their own, prescriptive requirements, thereby eliminating the pragmatic flexibility intended by the Directive. In the U.S., states such as Massachusetts and Nevada have enacted very specific, prescriptive laws that require affected businesses to follow pre-set security protocols. Microsoft believes that any privacy framework for the cloud should instead be built to evolve with technology and society through the years, and not set in a single moment in time. This more pragmatic approach is necessary not only to enable innovation and growth of the cloud, but also to provide consumers with meaningful privacy protections that are attuned to evolving consumer needs and expectations.

A. Governments should enhance legal certainty for cloud services.

Imagine driving along the highway and seeing two signs next to each other, one saying that the speed limit is 100 km/hr, another that it is 65 km/hr. Most drivers would find this both

²² FTC, *Protecting Consumer Privacy in an Era of Rapid Change - A Proposed Framework for Businesses and Policymakers (Preliminary FTC Staff Report)* (December 2010) <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>.

confusing and outrageous. Yet that is essentially the position that cloud service providers often find themselves in today.

Specifically, there is tremendous uncertainty about which jurisdiction's laws apply to data in the cloud and/or which jurisdiction can assert authority over the data (regardless of the law applied). Because of this uncertainty, cloud providers face substantial compliance burdens that drain resources away from the development of new privacy protecting solutions. This uncertainty also means that providers often cannot give the assurances customers deserve on matters such as the circumstances in which their data may be accessed by law enforcement or whether and for how long the provider is required by law to retain their data.

Within the EU, for example, the Data Protection Directive is unclear about which Member State's law applies to a provider offering online services to users in multiple EU markets. Lacking clarity, *all* of the Member States involved may take the position that their laws apply to a cloud service, forcing a provider to try to comply with local laws that impose divergent or even conflicting obligations. Microsoft therefore welcomes the European Commission's recent statement – issued as part of its consultation on an EU-level review of the Data Protection Directive – that it “will examine how to revise and clarify the existing provisions on applicable law . . . in order to improve legal certainty.”²³ We also welcome the Article 29 Working Party's recent suggestion that the EU determine a single applicable law for a given service using an approach similar to the “country of origin” principles found in other legal frameworks, like the EU's e-commerce rules.²⁴

Similar challenges exist in the U.S. For example, nearly every one of the 50 U.S. States has its own laws governing the circumstances in which a data breach notification should be sent to customers. Instead of this patchwork legal landscape, an issue as important as data breach merits a uniform law that applies across the U.S.

When combined with broad or conflicting assertions of jurisdiction, differences in substantive laws on key issues like data privacy, data retention, and law enforcement access also create irreconcilable obligations for cloud providers. For example, service providers may face situations in which the disclosure of data to one government in response to a lawful demand under that country's rules would violate the privacy laws of the country where the data is hosted or processed. This type of situation poses a dilemma for cloud providers in which it is impossible to comply with the laws of both countries asserting jurisdiction over the data in question.

While the ultimate goal should be global consensus on balanced and predictable rules governing data in the cloud (as discussed below), in the near term the U.S., EU and other jurisdictions each should take steps so that the law to be applied, the obligations that the law imposes, and the jurisdiction that will have authority over data is clear *within* their boundaries. In Europe, this requires fuller harmonization of national laws in each of these areas; in the U.S., Congress should enact legislation to preempt state laws that are inconsistent with a nationwide standard. By establishing clarity in this area, governments will better enable cloud providers to invest in developing new services

²³ See Section 2.2.3 of Communication on *A comprehensive approach to personal data protection in the European Union* COM(2010) 609 final, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

²⁴ See Article 29 Working Party Opinion 8/2010 on applicable law adopted on December 16, 2010 (WP 179), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

and to provide assurances to their customers as to how the law will affect the storage, processing, and use of their data.

B. Governments should make the law more results-oriented by ensuring that regulatory rules measure compliance against desired outcomes.

An outcome-based framework (*e.g.*, “companies must provide users with clear and easy-to-understand notice of their privacy practices, delivered in a manner appropriate to the nature of the online service”) will better serve consumers and industry than will a pre-determined set of means to reach that goal (*e.g.*, “companies must send all customers a written notice of privacy practices by postal mail”). By not freezing in time the means by which an outcome is achieved, governments can provide a robust level of protection for consumers *and* enable continued innovation by industry.

In the 1980s and 90s, regulators sometimes adopted rules that were appropriate for their era of computing but were designed with specific technology and means of implementation in mind. For example, in the U.S., the federal statute governing law enforcement access to user data, known as the Electronic Communications Privacy Act (ECPA), is remarkable in that it extends greater privacy protections to email messages stored for less than 180 days than to emails stored for more than 180 days. This approach may have made some sense when the statute was enacted in 1986 and online data storage was limited. But today, users keep email in the cloud for years – and expect that these emails will be just as private on day 181 as on day 179.

Proposed policies relating to user consents and cookies threaten to repeat this pattern of focusing on implementation rather than outcomes. In Europe, for example, some regulators – building on a requirement that users give informed consent to the deployment of cookies – have suggested that users should be required to affirmatively indicate consent (*i.e.*, opt-in) *every* time a cookie is deployed on a website that they visit. In practice, this would require users to tick dozens and sometimes hundreds of boxes during each online session – a process that is likely to lead to users opting *in* as a matter of routine, even where their privacy would be better protected by opting *out*. Regulators – and consumers – would be better served by an approach that required online service providers to obtain consent, but offered them latitude to innovate when determining how best to implement that obligation.

In the U.S., the FTC is contemplating a less extreme, but nonetheless concerning requirement that all browsers provide a “Do Not Track” feature. Under this regime – which the FTC concedes may still leave consumers uncertain as to whether their choices are being respected – browsers would need to be re-engineered and websites and ad networks modified to detect the new browser feature. Microsoft itself has created various browser-based solutions to promote privacy, including the InPrivate Browsing feature in IE8 and 9, and the new Tracking Protection feature in IE9. We do not believe, however, that browser-based mechanisms are the only means by which consumers can effectively control their online information, or that a single, browser-based mechanism should be mandated. Instead, by providing room for different means of designing and implementing solutions within and outside of the browser environment, regulators can promote innovation and allow providers to develop alternative approaches to protect data.

Indeed, there are many examples of how an outcome-focused framework can withstand the test of time, protect consumers, and leave industry breathing room to innovate. Consider the EU’s E-Commerce Directive, which sets forth a broad framework for e-commerce, including rules on information requirements, commercial communications, and e-contracts. Among other outcome-

focused rules, the Directive imposes transparency requirements by which companies engaged in e-commerce must provide users with the company's contact information in a way that is easily, directly and permanently accessible. Prices likewise must be indicated clearly and unambiguously. The Directive does not, however, dictate the specific *means* by which this information is to be communicated. This flexibility has allowed e-commerce companies to provide information in different ways depending upon the nature of the service or intended audience, while nevertheless ensuring a level of transparency that protects consumers from abuse or misleading practices.

Governments wisely have begun to consider proposals that would protect consumer privacy in the cloud through an outcome-oriented regime. Microsoft welcomes, for example, the European Commission's suggestion that an "accountability" principle be expressly included in the EU data protection regime. Under an accountability-based regime, data protection standards and requirements are enshrined in law, but individual organizations have much of the responsibility to determine how best to meet those standards in practice. It is important, however, that the benefit of an accountability approach not be squandered by simply imposing a requirement that organizations be accountable on top of the EU's existing prescriptive rules. Rather, accountability should be used *instead of* prescriptive rules.

In that same vein, Microsoft also welcomes the U.S. Department of Commerce's recommendation of legislation that would create a safe harbor from government enforcement actions for companies that adhere to appropriate voluntary, enforceable codes of conduct developed through open, multi-stakeholder processes. The Department of Commerce correctly emphasized that this flexible, safe harbor approach would not diminish protections for consumers, noting that "[f]ailing to comply with the voluntary, enforceable code's provisions could lead to an enforcement action by the FTC or a State Attorney General." Microsoft has long supported the notion that companies can fulfill statutory requirements by complying with an agency-approved safe harbor program that includes an enforcement mechanism to protect consumers.

C. To enhance innovation in the cloud, governments should facilitate movement of data across borders while maintaining legal protection for consumers.

Like the Internet, cloud services are global in nature. Being able to move data among large data centers in multiple geographic areas allows cloud computing providers to pool IT resources and consolidate overheads and purchasing power; this, in turn, results in significant cost and efficiency benefits for consumers, as well as the environmental benefits that flow from using fewer data centers.²⁵ From an operational standpoint, cloud computing providers move data between data centers in order to offer key services to customers, including 24 hour technical support and round-the-clock product development. Data transfer likewise is essential to data back-up and resiliency. As noted in a recent report by the Lloyd's insurance market, "The digital world is still susceptible to physical disasters such as flooding, earthquakes and hurricanes," and thus "geographic concentration" of data may increase risk of loss.²⁶ The cloud provides a perfect vehicle for ensuring that critical information does not disappear forever as a result of natural or man-made disasters.

²⁵ See Microsoft, *The Economics of Cloud Computing for the EU Public Sector*, *supra* note 8.

²⁶ "Digital Risks - Views of a changing risk landscape," Lloyd's Emerging Risks Team Report (October 2009) http://www.lloyds.com/~media/Lloyds/Reports/360%20Emerging%20risk%20reports/DigitalRisksreport_October2009v2.pdf

Rules governing the transfer of data and information across borders, however, do not accommodate the current realities of broadband-enabled computing. While not their intention, these rules limit the innovation and economic development otherwise made possible by the cloud, and often do not produce any corresponding benefit to consumer privacy. As the European Commission has recognized, “there is a general need to improve the current mechanisms for international transfers of data” in light of the vastly increased delivery of services over the Internet since the Data Protection Directive was adopted 15 years ago.²⁷ The Directive as it now stands broadly restricts the transfer of personal data from within Europe to any country whose domestic laws do not provide a level of protection that the EU considers “adequate.” In practice, only those countries – less than 10 to date – that provide the same precise methods of protection as the EU have been deemed adequate. Other governments go even further and impose near-complete bans on certain types of data transfer, such as in Nova Scotia and British Columbia. There, most personal data held by public bodies cannot be moved to any jurisdiction outside of Canada.

Regardless of the nature of an unduly strict cross-border data restriction – whether it is the result of an express prohibition on data export, a limitation based upon an adequacy requirement, or inconsistent laws across jurisdictions – the unintended consequence is to depress investment, reduce trade, and deprive consumers and enterprises of the benefits of cloud computing and other innovations. Cloud service providers subject to inflexible cross-border data restrictions are forced to implement cumbersome and expensive processes in order to legitimize the data transfers, even when more pragmatic procedures could provide the same or even a better level of protection to users. Alternatively, the provider may be forced to store the data locally in the jurisdiction that imposes the export restriction, thereby preventing the provider from being able to offer customers the cost and efficiency benefits that stem from being able to move data to multiple geographic areas, and eliminating the potential energy efficiencies and environmental benefits of consolidating resources in fewer data centers.²⁸ In a nutshell, the desire for local data centers is in conflict with the efficiencies associated with the scale economics of cloud computing.

Europe and other jurisdictions reviewing or considering privacy frameworks may find a helpful model in the “accountability” approach taken by the Canadian federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA). Under PIPEDA, the organization transferring data for processing takes responsibility and remains accountable for its protection and appropriate use – regardless of whether that data is transferred across borders. The APEC Privacy Framework in Asia takes a similar, accountability-based approach. These approaches provide for transfers of data in a way that is secure but free of bureaucratic hurdles that inhibit data flows essential to cloud-based services.

IV. Governments and industry have opportunities to build on practices that have worked in the past and can be successful in the future.

History has demonstrated the potential for success when industry, users and government work together to adapt legal frameworks and practices to new technologies. Two examples from Europe – the adoption of the Software Directive in 1991, and the 2007 revision of the broadcast-focused Television Without Frontiers Directive – are instructive.

²⁷ See Communication on *A comprehensive approach to personal data protection in the European Union*, *supra* note 23.

²⁸ See Microsoft, *The Economics of Cloud Computing for the EU Public Sector*, *supra* note 8.

Software Directive. Prior to the 1980s, for the most part software was a product that was closely integrated with hardware and services sold by a few large firms (*e.g.*, Wang, IBM) to other businesses. By the mid-1980s, however, advances in microprocessor technology and the embrace of an “open innovation” business model had brought about the personal computing revolution and the rise of a diverse software industry serving the mass market.

This transformation brought the power of information technology into the lives of ordinary citizens. At the same time, it quickly became apparent that the existing legal structure in Europe (and elsewhere) lacked protections necessary for the software industry to reach its full potential. Most notably, in many Member States software did not fit clearly within existing understandings of what could and could not be protected by copyright – resulting in vastly different degrees of protection for software across Europe. This uncertainty undermined incentives for investment in software innovation.

Beginning in the mid 1980s, software developers and other industry stakeholders urged legislators to provide more clear and consistent copyright protection for software in Europe. European policy makers heeded calls for reform and, working with industry and users, in 1991 adopted the Software Directive – a harmonized, balanced framework for copyright in software that works as well today as it did on its adoption 20 years ago. The Directive and similar measures eliminated a broad range of disparities and uncertainties between Member States’ laws, and enabled software companies to create a genuine single market for software in Europe, reducing inefficiencies in product distribution and lowering prices for customers. In part as a result, the software industry in Europe has grown dramatically between 1991 and today, and now accounts for over half of the employment in IT in Europe.

Audiovisual Media Services Directive. In 1989, the EU adopted the Television Without Frontiers (TWF) Directive with the goal of developing a pan-European single market for broadcast and cable television. By all accounts, the TWF Directive achieved its goals through introduction of harmonized rules and minimum standards for the transmission of television programming across national borders. However, the TWF Directive was written specifically to apply to a single, specified medium: the delivery of linear television services by cable or over the air using the radio spectrum. It therefore was not prepared to accommodate the technological convergence that began in the 1990s with the public introduction and rapid growth of the Internet, as well as the deployment of advanced wireless networks, non-linear viewing options like cable Video on Demand (VOD), and similar innovations for the distribution and consumption of audio-visual media.

Aware of the TWF Directive’s limitations, starting in the mid 1990s some European policymakers proposed amendments to reflect convergence trends and the fact that the same content regulated by the TWF Directive was also being delivered over the Internet outside of that framework. Initially these efforts to extend the Directive to non-broadcast services were rejected, but over time various industry actors worked with regulators and other stakeholders in search of a balanced regulatory framework attuned to evolving technologies. Among other steps, various expert groups were formed through which industry was able to debate and provide practical, technical, and market-based guidance to legislators concerning key aspects of the Directive’s revision, including its scope and application to new media services.

The resulting 2007 Audiovisual Media Services (AMS) Directive takes a technology-neutral approach that focuses on the type of service provided to consumers rather than the particular platform on which it is delivered. Within this framework, a program that is webcast over the Internet is subject to broadcast-like regulation, in contrast to a program that is made available for download on the

Internet. The end result is a flexible regulatory framework that accommodates new audiovisual platforms and services, and applies to them certain common policy objectives, such as the protection of minors.

Just as government and industry stakeholders came together to update legal frameworks to reflect evolutions in audiovisual services and software, today governments in Europe, the U.S. and around the world have the opportunity to maintain or strengthen privacy and security protections while removing legal inconsistencies and uncertainties that constrain growth and adoption of cloud computing. By collaborating with industry, governments can build a legal framework for the cloud that enables the creation of new jobs and economic growth at the same time that it protects the privacy and security of data in the cloud, provides tools to combat cybercrime, and promotes competition and consumer choice.

V. Governments also should work together towards a global framework for cloud computing.

In addition to working to harmonize laws and facilitate data flows from within their own borders, governments should work across borders towards a global framework for the cloud. No government on its own can solve challenges to broader deployment and adoption of the cloud. Only through government-to-government collaboration can they create the consistency among regulatory frameworks that is necessary to make the cloud work. Governments could begin by working to develop rules that will facilitate data flows across national and regional borders. Alternatively, governments could work together to develop and agree upon shared principles for determining when a country has jurisdiction over data stored in the cloud.

It may prove most effective for governments over time to seek a multilateral framework on these issues in the form of treaties or similar international instruments. While this option undoubtedly would require significant diplomatic leadership and resources, it offers perhaps the best hope of addressing legitimate government needs in a coherent fashion while ensuring that business and consumer interests in privacy are met on a global scale. Countries could work within entities such as the G8 or G20 to take up this issue, and rely on multilateral organizations such as the OECD to research the problems faced and make recommendations for how to resolve them.

A less formal option would be for countries to engage on a bilateral or regional basis in consultations and consensus building to better harmonize their respective data protection regimes and better resolve data access issues. Such engagement can increase awareness of the problems and pave the way for a longer-term, more formal solution. For example, in Asia, progress made on the ASEAN-Australia Development Cooperation Program on harmonizing e-commerce legal frameworks and the APEC Privacy Framework and Pathfinder Projects provides a solid platform for further development and addressing of the divergent jurisdictional approaches to technology policy. Such multi-party, regional discussions offer an opportunity to boost cloud computing and expand its benefits on many levels across a region.²⁹

It is especially important that the EU and U.S. pursue transatlantic initiatives focused on the cloud. These discussions could proceed in a manner similar to bilateral agreements that they have negotiated in other fields, like air transportation services and agriculture. A common approach to the

²⁹ For more information on these respective initiatives and frameworks, see <http://www.asean.org/aadcp/whatisaadcp.html> and <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx>.

cloud on both sides of the Atlantic could also serve as a model for future negotiations elsewhere. If, instead, either the U.S. and/or the EU turn inward and fail to coordinate their actions in this area, there is a danger that the law will diverge between the two sides of the Atlantic – leaving, in effect, a gap in the cloud that would take many years to bridge.

Cooperation and coordination also are important to secure the cloud from cybercrime and related concerns. Fighting cybercrime always has been a global issue, but cloud computing makes it more so. With a victim often in one jurisdiction, the datacenter or centers in other jurisdictions, and the perpetrator in yet another jurisdiction, there must be an effective mechanism for cooperation among law enforcement agencies in the EU, U.S., and elsewhere. There is a need for clear and consistent standards for production, retention and preservation of data in investigations that concern multiple jurisdictions; investment in technological know-how for local law enforcement; and cooperation in the establishment of international clearinghouses, through which data on cybercrimes is shared with a central point of global contact to evaluate trends and make connections that will help identify perpetrators.

VI. Conclusion

To bring about the economic growth and societal benefits that cloud computing offers, governments and industry must work together, just as they did in fostering past eras of IT-driven growth. Microsoft is committed to doing its part, both through our market-leading privacy and security practices and through support of legal reform. Already in Europe, the U.S., and other jurisdictions, governments have begun to map out necessary measures in consultation with a broad array of stakeholder groups. We are encouraging governments to revisit regulatory frameworks as needed, and provide greater certainty *within* their borders, as well as to engage in bilateral and multilateral negotiations to liberalize the movement of data in the cloud and ensure more harmonized protection of that data. Perhaps most importantly, we continue to invest heavily to bring the benefits of cloud computing to people and organizations around the world.

For more information please contact publicpolicy@microsoft.com or visit www.microsoft.com/publicpolicy.

Microsoft[®]