Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing

Introduction

Cloud computing offers the potential for efficiency, cost savings and innovation gains to governments, businesses and individual users alike. And because the cloud transcends national boundaries, cloud computing also offers a unique opportunity to bring Europe one step closer to achieving the EU 2020 vision of a robust, truly integrated and seamless Digital Internal Market.

To realize these benefits, there are also challenges that must be addressed along the way – enabling wide-scale cloud adoption by giving users the confidence needed to embrace cloud computing. Some of these challenges call for industry action, some require government action, and many will involve active collaboration of consumers, industry and government. This paper is intended to explore some of these issues, particularly those that touch on regulatory differences between countries where more harmonization and government coordination or legal reform is needed. The call to action presented includes proposals that will need careful consideration and an open and inclusive debate, and Microsoft looks forward to a constructive dialogue with users, policymakers and innovators on the subject.

Equally important are many aspects of cloud computing involving the relationship between consumers of cloud services and the many providers of cloud services, or among cloud providers themselves – issues such as service level agreements, interoperability, and transparent business practices. These discussions are getting considerable attention as customers voice their needs, and the marketplace is both active and competitive in attempting to meet these needs. This marketplace includes many customers and many vendors, that are large and small, and that come from every country and region. Europe can take full advantage of this heterogeneous and vibrant marketplace and reap the benefits of this wave of computing by removing the obstacles that could reduce confidence in the use of cloud services and slow the uptake of cloud computing.

Responsible government action includes ensuring that Europe has the right communications infrastructure in place to support the cloud; creating a sensible and coherent EU regime governing the flow and protection of data stored in the cloud; and establishing and enforcing an advanced privacy and security framework that is more closely aligned with the ways in which computing is evolving.

The digital agenda is now squarely at the centre of Europe's priorities, and with a new Parliament underway and a new Commission soon to be in place, this is an ideal time to initiate a multi-stakeholder dialogue about the cloud. This paper is intended as Microsoft's contribution.

I. The Promise of Cloud Computing

In Europe and elsewhere, computing is experiencing a powerful transformation. Driven by innovations in software, hardware, and network capacity, the traditional model of computing – where users operate software on their own PC and IT systems – is gradually being replaced by one where users increasingly combine ever-smarter client devices that access applications and services both on the client itself and over the Internet, i.e., “the cloud”. In terms of efficiencies, innovation acceleration, cost savings, and greater computing power, there are substantial benefits to be gained from cloud computing.

European businesses, particularly SMEs, already are taking advantage of this combination of client and cloud to innovate, to reach wider markets, and to become more competitive. At Microsoft, we have seen this first-hand; many of the 8,000 startup IT companies in the EU involved with our BizSpark programme, among the 126,000 European partners overall that we work with, are directly involved in developing new cloud technologies and cloud-based services. New companies such as Lokad in France, TradeFacilitate in Ireland, Huddle in the UK – all are defying slow economic times to build new businesses looking to the future. European governments and citizens, meanwhile, are also exploiting the cloud, with many public services now being offered at less cost and with greater speed to more individuals.

These are among the many reasons why Microsoft is excited about the emergence of cloud computing and collaborating closely with European innovators. It is also why we are investing heavily in the cloud infrastructure, an open and interoperable platform, and products and tools that maximize user flexibility, security and choice to ensure a seamless computing experience.

II. Challenges to the Growth of a Digital Internal Market for the Cloud

Commissioner Reding stated recently that the “protection of personal data . . . and the ability to preserve private information are of major importance to guarantee trust in an online single market”.[1] This rings particularly true with regard to cloud computing.

Many experts, including those at Microsoft who collaborate in different platforms (like ENISA) agree that the cloud offers important opportunities to advance security. For example, most cloud computing providers have greater and better security expertise, management and controls than many enterprises and even many government agencies. But at the same time, the cloud infrastructure also gives rise to new privacy and security challenges, and presents attractive targets for hackers. The cloud will move data from local on-site PCs and servers to equipment that is physically and administratively controlled by a third party and that may be located in third countries. This shift from the desktop to the cloud raises many issues, among them what third parties can (and are legally obligated to) do with the information and who can access it.

Industry has an important responsibility to pursue initiatives that enhance privacy and security in the cloud, both by adopting robust practices and technologies that effectively protect data online and by clearly communicating these measures to users in order to enable them to make informed choices. Initiatives such as Trust in Digital Life are going some way to address these issues. Governments have a role to play here as well. Part of this role requires the creation of a sensible and coherent regime in Europe governing data stored in the cloud, so that cloud users and cloud providers have a clearer understanding of what rules apply and how. And part requires the establishment and

[1] Viviane Reding, Member of the European Commission responsible for Information Society and Media, A European Digital Agenda for the New Digital Consumer, BEUC multi-stakeholder Forum on "Consumer Privacy and Online Marketing: Market Trends and Policy Perspectives" Brussels, 12 November 2009, SPEECH/09/524.

enforcement of a advanced framework of privacy and security that is more closely aligned with the ways in which not only computing, but also the interaction between people, is evolving.

Privacy and security are, of course, not the only prerequisites to a robust and seamless cloud market in Europe. Technological elements are also important. Continuous and affordable broadband access, for example – achieved through traditional and wireless technologies and more efficient use of spectrum – is essential to enable ubiquitous access to the cloud.

III. A Call for Industry and European Action

Before the benefits of the cloud can be fully realized and a true EU Digital Internal Market created for European SMEs and other stakeholders, both industry and European policy makers need to take responsible action to address both the capability of all Europeans to connect reliably with cloud technologies, and to enhance their confidence in using them. Our efforts should focus on:

- ***Ensuring that the European communication infrastructure is cloud-ready.*** Cloud computing can only deliver the full benefits when there is ubiquitous and affordable broadband access. Continuity of access will encourage consumers to make greater use of cloud computing services and SMEs to focus more on developing new content and services.

- ***Ensuring a genuine single market by bringing coherence to the legal framework applicable to the connected world, including the cloud.*** This is needed to avoid data of European citizens and cloud providers being subject to a fractured and, at times, conflicting set of legal rules and principles. Among other things, Europe should work to address and eliminate divergent Member State interpretation and application of data retention and other e-communications rules.

- ***Ensuring greater transparency about the privacy and security practices of cloud providers*** through industry adoption of a self-regulatory code, alongside possible reforms to the European framework for international transfers, in order to ensure that essential privacy protections apply to the cloud and users can make informed choices.

- ***Enhancing security in the cloud*** by providing for greater rights of civil enforcement against cyber attacks and ensuring greater coordination and resourcing for law enforcement bodies.

In addition, the EU should ***take a leadership role*** in the adoption of a multilateral framework in the form of a treaty or similar international instrument to resolve persistent problems of jurisdiction and sovereignty over multiple aspects of the cloud.

A. Ensure that the European communication infrastructure is cloud-ready

Increasing connectivity demands arising from the emergence of cloud computing technologies have reinforced the importance of enhancing Europe's broadband infrastructure. Confidence in cloud computing begins with pervasive and reliable connectivity.

The EU has recognised the need for improved broadband, placing it squarely in Europe's digital policy agenda. And the Commission has already devoted significant attention to creating a framework to encourage investment in next generation access, which will see optical fibre move closer to consumer homes in order to enhance access network performance. While optical fibre will play an ever-increasing role in the cloud-ready infrastructure, however, wireless technologies are also crucial to ensuring that the benefits of cloud computing will be widely available – including in remote and rural areas.

Spectrum regulators can assist in achieving ubiquitous access by encouraging radically more efficient use of spectrum. The key bottleneck for the deployment of wireless technologies is the lack of available spectrum suited to wide area coverage. European spectrum policy has proved contentious, demonstrated by the Commission's two year effort to define and implement a pan-European Digital Dividend under which spectrum would be released from broadcasting to support wider broadband connectivity. It is encouraging that the Commission has now set itself the goal of streamlining spectrum policy development through a multi-annual programme, bringing together the Commission, Parliament and Council.

A priority for this multi-annual programme should be the TV white spaces – the gaps left between TV stations. These represent substantial underused capacity which could form a powerful complement to spectrum released under the Digital Dividend, helping to achieve the ubiquitous access needed for cloud computing to deliver its full potential for European citizens and consumers.

B. Ensure a single market and promote cloud innovation and use through a more coherent regulatory framework

As cloud computing evolves, the traditional geographical limitations applicable to data flow increasingly disappear. Information can be created in France using software hosted in Poland, processed in the UK, stored in Ireland and accessed in Latvia by Italian citizens. Cloud providers, meanwhile, may have operations and data centres located in different countries within Europe and across the globe, further contributing to cross-border storage and dissemination of data for an increasingly mobile user community – as exemplified by the take-up of mobile services in Europe.

In this way, cloud computing provides the hardware and software infrastructure and enables the creation of a truly single market for digital services in Europe. But, this digital single market can only succeed if Europe fosters a harmonized and coherent legal regime to govern the flow of data, including access, retention, and protection. Unfortunately, this is not the case in Europe today; on the contrary, the legal frameworks governing the cloud and other connected technologies are fragmented and inconsistent, and they risk erecting new barriers to the single market. Europe's data retention regime – which flows from the EU's Data Retention Directive – illustrates the problem.

The Data Retention Directive generally requires providers of electronic communications services ("ECSs"), including those operating via the cloud, to retain certain categories of communications and traffic data, such as the email address of the recipient of an email or information identifying the recipient of an Internet voice call, from anywhere between 6 months and 2 years. These retention mandates are meant to enable law enforcement authorities to access and review in criminal investigations the communications data that might otherwise have been deleted by the ECS.

Unhelpfully, Member States have taken divergent views as to whether cloud service providers need to retain data under the Directive and, if so, for how long. For instance, Member States disagree on what Internet-based services constitute ECSs; indeed, in some cases even authorities *within* the same Member States disagree. Even assuming there is agreement on when a provider is an ECS, some Member States have extended data retention obligations to services beyond those encompassed by the Directive. These problems are compounded by the latitude Member States have under the Directive to adopt varying retention periods (from 6 months to 2 years), which are all too frequently applied to the same service provider with unfortunate results. A provider's compliance with a 6-month retention mandate of one country may violate a 2-year mandate arising in another.

The result is that cloud providers continue to operate in a realm of legal uncertainty, unsure of their obligations and often expected to comply with irreconcilable data retention mandates. Cloud users face similar uncertainties.

As a first step toward the creation of a Digital Internal Market for the cloud, there needs to be agreement on which services constitute ECSs across the Member States. This is, of course, a challenging task, particularly given that cloud offerings can include other services alongside electronic communications services – but it is a question that must be tackled quickly. The Commission – and possibly the newly-launched Body of European Regulators for Electronic Commerce (BEREC) – should as a matter of urgency work with stakeholders to clarify this issue so that cloud providers know and understand their obligations to achieve the shared goal of meeting the emerging needs of European citizens and consumers.

Clarifying when a cloud provider is an ECS is only one part of the solution. To the extent the Directive is interpreted to apply to certain cloud provider services, efforts also are required to address inconsistent Member State data retention mandates. One possible solution could involve amending the Directive to introduce a single, uniform period for data retention that applies in each Member State. Alternatively, a system of mutual recognition could be established whereby the courts and regulators in one Member State recognize and honor the period chosen by another Member State as long as it conforms to the Directive. Member States could continue to choose a retention period ranging from 6 months to 2 years, but would refrain from applying their own period to data stored by providers in another Member State.

The Commission's ongoing review of the Directive's implementation provides an ideal opportunity to consider and resolve these issues. We hope that the Commission will work expeditiously along the lines it has started, and with the full range of stakeholders, including cloud users and providers, law enforcement, data privacy authorities and Parliament, in the effort to understand and resolve the challenges of the current regime.

Addressing the challenges surrounding data retention is only the first step in providing a harmonized and coherent legal framework for cloud users and providers, however. Similar national divergences exist in other regulatory frameworks affecting the cloud, including the rules relating to e-privacy, network security, and e-communications. Confronting these emerging issues and crafting holistic solutions must become a top priority for European policymakers if the vision of the Digital Internal Market is to become a reality.

Fortunately, the EU has shown itself adept at anticipating technological transitions and shaping its legal frameworks accordingly. In the late 1980s, for example, European policymakers recognized that diverging legal rules relating to the copyrightability of software in EU Member States threatened to stifle software development in Europe at a time when software innovation and use was poised to explode. In 1991, the EU adopted the Computer Programs Directive, harmonizing the copyright regime and creating a single market for software across Europe, enabling Europe's software sector to flourish. With Europe now reaching another transitional point in computing, diverging rules as described above present a similar risk; the Lisbon Treaty and related initiatives such as the Stockholm programme already in the pipeline provide the EU with an opportunity to realign and harmonize its laws.

C. Promote transparency and privacy for consumers and businesses in the cloud

In order for the cloud to realize its full potential, users must be able to repose their trust in it; users should not feel that to obtain the benefits of the cloud they need to sacrifice their own control over their data and the privacy or security of it. The success of the cloud depends on ensuring that its use does not lead to an erosion of the user's fundamental rights or limitations on their ability to store, access, process and move their own data.

While cloud providers recognize the importance of user confidence, they differ in their approaches to privacy and security. This may reflect different business and revenue models; whether the provider traditionally has focused more on consumers as opposed to enterprises or government customers; differing assessments of how best to mitigate and manage security risks; and other factors particular to that cloud service provider. These varying approaches are not inherently problematic; to the contrary, this may provide one important way by which cloud service providers can distinguish their offerings to potential customers, on mutually agreed minimal conventions.

What is problematic, however, is that the privacy and security practices of cloud providers often are not transparent to the user. European data protection regulators have noted the problem, having expressed concern with the opaque and uninformative privacy policies and statements used by online service providers. While all providers claim that they respect their users' privacy and have appropriate systems in place, few back up these claims with the specifics that enable users to evaluate these claims or to compare privacy practices in any meaningful way. The challenge is to ensure users receive more and better information from cloud providers about how their data will be stored, processed and made available, as well as learn what measures are being taken to secure their data in the cloud.

This challenge can be overcome. Cloud providers clearly have a responsibility to provide better information than they do at present to explain how data are collected, stored and processed, so that users can make informed decisions about their options. Simply put, it should not be enough for service providers to simply say that they respect users' privacy; there needs to be real transparency about what they are actually doing to protect that privacy. This increased information flow needs to be accompanied by steps to ensure that users understand the information being provided – including, for example, whether a provider's architecture, infrastructure, and related information security controls satisfy verifiable and robust security criteria. Cloud providers should engage with other relevant stakeholders, such as consumer groups and data protection regulators, on how best to educate users on privacy and security matters.

One potential solution could involve industry's adoption of a new self-regulatory code on a set of agreed "*Transparency in Cloud Computing"* principles – principles designed to ensure that users are able to make informed decisions when selecting their service provider. For example, service providers could be required to explain their data handling practices in clear and precise terms, set out their policies relating to data portability and user access, and clarify how long user data are retained after an account is terminated. Critically, this could also ensure that providers explain whether their information security programs comply with leading third-party standards, such as the International Standards Organization series (ISO 27000) for information security management or similar requirements; whether they utilize appropriately robust authentication mechanisms; and whether applications and other components of the service (both hardware and software) receive thorough security testing before deployment. ENISA's recently-released Information Assurance Framework for cloud providers could help in determining the criteria that might be included in any Transparency in Cloud Computing principles.

While industry is working to provide greater transparency, policymakers at the same time need to ensure that Europe's existing data privacy regime and its solid protections apply sensibly to the cloud and take account of the advances in computing made since the regime first came into existence. Unfortunately, the EU's data protection framework, enacted to regulate an earlier era of computing involving point-to-point data transfers, appears increasingly out-of-date in a world of routine cross-border and flexible, adaptive international data flows predicated on cloud architectures. To the extent that framework cannot sensibly be applied to the cloud and similar connected technologies, then there is a real risk that the framework will come to be seen as impossible to implement, its requirements henceforth ignored and the privacy rights of European citizens threatened.

Already, many have questioned whether key instruments, such as the Data Protection Directive, can be sensibly applied to services in the cloud in practice. Many feel they cannot, pointing for instance to weaknesses in existing provisions regulating transfers of data outside the EU. The trend toward cloud computing and the growth of online services has resulted in a dramatic increase in data flows. The current mechanisms did not foresee this, and they are too inflexible and cumbersome to be applied to current needs. For this reason, the Commission's decision to review the Legal Framework for Data Protection could not be more timely; it has triggered a vigorous and healthy debate on whether the European data protection framework fits this new world of cloud computing.

Among other things, the Commission should consider more efficient mechanisms for international data transfers. Ensuring continued strong protection for EU-origin personal data, regardless of location, should continue to be the objective of EU rules on international transfers. However, existing mechanisms for doing so may need to be improved as companies must now routinely transfer data to jurisdictions outside of the EU that are not deemed to offer equivalent protection for personal data. By critically examining the European data protection regime in light of the specific challenges of the globally connected world and the cloud, Europe can ensure that its data privacy regime remains fit for purpose, guiding companies on how to comply with data transfer provisions and continues to provide world class privacy protections for future generations of Europeans. Europe could also be at the forefront in the development and – more importantly – adoption of Privacy Enhancing Technologies (PETs).

D. Enhance security for data that are held in the cloud

Microsoft has a long history of supporting law enforcement to help fight digital crime, including crimes involving data in the cloud. In our experience, three elements are critical to combating digital crime successfully: (1) strong deterrence through criminal and civil enforcement with meaningful penalties and remedies; (2) a legal framework that encourages cooperation and information-sharing between the public and private sectors, especially the sharing of technical expertise; and (3) the ability for law enforcement in different jurisdictions to team up and exchange information globally.

Unlike other regions, many of these elements are already in place in Europe. A major exception, however, remains in the area of civil enforcement. Under many Member State laws, only the party whose individual account is directly harmed by a cyber attack can bring a legal action against the perpetrator of the attack. This means that cloud service providers and other online intermediaries are prevented from instituting such actions in their own right on behalf of their customers, even though they have a clear stake in preventing future attacks. Microsoft believes that the security of cloud computing services would be greatly strengthened by changing these laws to give third parties a right of action against hackers and other cyber criminals.

The absence of third-party rights to bring claims in cases of cyber attacks hinders robust enforcement, since in many cases the individual party affected may be unwilling or unable to pursue a claim. One of the many positive attributes of cloud computing is that it provides cost-effective, scalable services, enabling SMEs to reap the benefits of advanced ICT infrastructure that previously were only affordable for large companies. SMEs are unlikely, however, to have the technical know-how, time, or money to take action against cyber criminals, who are frequently part of large-scale organized crime groups operating across borders.

A third party cause of action against hackers also would serve to complement the strong criminal prohibitions against hacking and related activities found in the EU's Framework Decision on Attacks against Information Systems. These strong criminal prohibitions would also benefit from robust enforcement in practice. Microsoft is concerned, however, that law enforcement efforts in the online space are often under resourced, and has initiated cooperation to build an effective and strategic public/private partnership to build capacity against cybercrime. The recent allocation by the European Commission of EUR 3 million to the 2CENTRE project, which has been undertaken by Ireland, France and Microsoft, is a positive step along these lines, representing the largest investment to date from the European Commission on a cybercrime project.

The need for enhanced law enforcement training, the development of expert forensic analysis related to computer crimes, and the deployment of state-of-the-art technologies capable of keeping pace with evolving threats is greater than ever. The ability to identify perpetrators of online attacks is one of the most fundamental challenges facing the international law enforcement community today. It is a challenge that will only increase as more data moves to the cloud.

E. Resolve sovereignty issues in the cloud through common approaches to jurisdiction

As the cloud evolves, and as users and providers begin to process and store greater amounts of user data, they face a growing dilemma. National authorities, confronted with the challenge of online crime and the use of the Internet in connection with threats to public safety or national security, increasingly are focused on obtaining access to user content and other data held by cloud service providers. Multiple jurisdictions may have an interest in a single matter, each seeking access to user information. There are, however, no universally agreed rules governing such access by law enforcement – and even in the EU, the rules are often unclear in their scope and application. The result is that service providers are increasingly subject to divergent, and at times conflicting, rules governing access to and jurisdiction over user content and data.

This thicket of competing and conflicting laws within the EU and internationally presents a significant obstacle to the delivery of cloud services that meet users' reasonable expectations of privacy. Where the rules of different nations within the EU and abroad conflict, a cloud provider's decision to comply with a lawful demand for user data in one jurisdiction may place a provider at risk of violating the privacy or other laws of another jurisdiction. Equally troubling, this situation makes it extremely difficult for providers to give their customers accurate and adequate notice of the conditions under which their data might be accessed by law enforcement.

Countries have sought to establish procedures to avoid such conflicts, via mechanisms such as mutual legal assistance treaties ("MLATs") and letters rogatory. But these mechanisms, which often have their origins in the nineteenth century, have proven problematic in practice. MLATs, for example, are too slow and cumbersome to capture electronic data stored on Internet servers, and law enforcement authorities in some cases are unwilling to pursue this route and expect prompt disclosure of data. And, although nearly four dozen countries have ratified and/or signed the Council of Europe's Convention on Cybercrime which requires signatories to establish points of contact who are available 24/7 to process requests, this has not resolved the problem.

In the EU, the recently-adopted European Evidence Warrant ("EEW"), which allows for the recognition of one Member State's evidentiary warrants in other EU Member States, provides a simplified, more expeditious system for the gathering and transfer of evidence in criminal proceedings. However, the EEW does not solve the issue for most cloud-based data. This is because EEWs cannot be issued to obtain communications data retained by providers under the Data Retention Directive or real-time intercepted communications.

These challenges – which are compounded by similar, but even more marked jurisdictional conflicts at the international level – have encouraged some countries to begin to ignore established procedures and simply demand that local employees disclose data regardless of where the data are located or where the relevant service provider is established. To encourage continued investment in cloud computing services and related technologies, there must be greater clarity and consistency on rules that will protect the privacy and security of user data while also ensuring legitimate law enforcement needs are addressed.

Industry has tried to take the initiative to help resolve these dilemmas, or at least lessen their impact. Microsoft, for example, has adopted a policy of responding to law enforcement demands to block access to Windows Live Spaces content only if it receives official written notice from a government indicating that the material violates local laws. More broadly, the Global Network Initiative (GNI) – a coalition of private-sector companies, investors, and human rights organizations – has promulgated voluntary guidelines for companies to follow in determining how to respond to government demands for access to (or censorship of) user data.

Helpfully, the Commission also has recognized the limitations of existing legal instruments for obtaining evidence in cross-border cases and the desirability of replacing them with a new single instrument. The recent Commission Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility hopefully will serve to open an important dialogue on this issue. More broadly, the changes in competence introduced by the Lisbon Treaty and the efforts to improve cross-border law enforcement cooperation under the Stockholm Program also provide opportunities to create greater coherence in this area.

Because the EU necessarily must address the jurisdictional challenge in order to facilitate criminal investigations across its 27 Member States, it is in an ideal position to take a leadership role in a transatlantic, and ultimately global discussion on this issue. One ambitious, but also the most effective, avenue for a solution would be for the EU to seek a multilateral framework in the form of a treaty or similar international instrument. While this option would undoubtedly require significant diplomatic leadership and resources, it offers perhaps the best hope of addressing legitimate government needs in a coherent fashion while ensuring that consumer and business interests in privacy and freedom of expression are adequately met on a global scale.

Whatever path the EU follows to resolve these issues, it is essential that its deliberations include not only representatives from law enforcement and justice, but also representatives of industry, consumer groups, and other interested stakeholders. Cloud computing will only reach its full potential if providers can establish data centres and offer services in multiple jurisdictions and cloud users can enjoy the benefits of these services without fear that each step will invite competing claims of jurisdiction and government access to data. The rules must balance the legitimate needs of law enforcement, users and industry, and it is vital that all stakeholders are represented in any deliberations.

*   *   *

Conclusion

If Europe is to reap the many economic and social benefits offered by cloud computing, it is imperative that European consumers, business, and governments have cause for confidence in the cloud. In short, cloud users must not be compelled to make a trade-off between flexibility and efficiency on the one hand, and privacy, security, and reliability on the other.

Industry is deeply engaged in developing solutions to these challenges. EU institutions and European governments too have a critical role to play, by working with stakeholders to ensure the necessary infrastructure is in place and the regulatory regime – both in Europe and internationally – is coherent, up-to-date and aligned with current technology.

With the benefit of a modernized technological and regulatory framework, European industry will have the solid grounding to deliver on the promise of cloud computing and once again expand the boundaries of innovation. Microsoft is committed to being part of this effort and looks forward to working with other stakeholders to achieve these goals.

Brad Smith

General Counsel, Microsoft

Brussels, January 2010