

BSA Computing Policy Agenda for 2011 in Europe

Introduction

In light of the European legislative agenda for 2011 - 2012, the Business Software Alliance has compiled a set of 10 concrete recommendations to ensure that the right policy environment is in place for development and adoption of cloud computing in Europe.

We believe these 10 policy actions – some legislative, others not - are essential elements of a comprehensive cloud computing policy framework in Europe needed to boost users' privacy and security in the cloud, promote the development of necessary standards and infrastructures, and ensure the clarity necessary to promote investments in cloud computing technologies.

BSA Cloud Computing Policy Agenda for Europe

- 1 Promote Transparency about Security Practices in the Cloud**
- 2 Enhance Data Breach Legislation**
- 3 Create Third Party Rights of Action Against Cyber Attacks**
- 4 Deter Hackers with Meaningful Penalties at National Level**
- 5 Harmonize Europe's Data Protection Framework at Member State Level**
- 6 Clarify the Application of Data Retention Rules across the EU**
- 7 Pursue Bilateral or Multilateral Cooperation on Protections for the Transfer of International Data and Assess Existing Mechanisms for the Processing of International Data Transfers**
- 8 Clarify the Application of Trade Disciplines to the Delivery of Cloud Services**
- 9 Foster Data Portability through Market-led and Technology-Neutral Policies**
- 10 Create and Enforce Provisions to Prohibit the Theft of Intellectual Property through Cloud Computing Services**

Promoting Security

The adoption of cloud computing by businesses and consumers is reliant upon the availability of information upon which to judge whether particular cloud services are secure. Cloud providers should provide information about their security practices to enable customers to make informed decisions. This should be accomplished through self-regulation initiatives such as the “Cloud Computing Information Assurance Framework” recently recommended by ENISA¹

The current revision of the legal framework on data protection in Europe provides an opportunity to extend the breach notification obligation to cloud computing providers, thus strengthening users’ protection – and confidence - online. The current European breach notification regime (introduced recently under the e-Privacy Directive (2002/58/EC) only for providers of electronic communication services) could be extended to providers of cloud services.

Combating Fraud

Illegal activities affecting cloud computing environments such as theft, fraud and malicious hacking are a threat to cloud users and service providers. Despite the Framework Decision on Attacks against Information Systems (2005/222/JHA) which enable Member States to impose criminal sanctions for cyber attacks, cloud users and service providers have no civil right of action against cyber criminals and intruders. Cloud computing providers and customers could play a more active role if they were granted a specific civil cause of action against intruders, coupled with meaningful statutory remedies.

In addition, effective deterrents against cloud hacking-related offences are required at national level so as to recognize the proportionality of harm caused by cyber attacks on data centres where multiple users’ data are stored.

Calls to Action

1 Promote Transparency about Security Practices in the Cloud

- Encourage voluntary industry compliance with the “Cloud Computing Information Assurance Framework” as recommended by ENISA

2 Enhance Data Breach Legislation

- Expand the existing European breach notification regime to all businesses, including cloud computing providers

Calls to Action

3 Create Civil Rights of Action Against Cyber Attacks

- Introduce a third party civil cause of action against intruders, coupled with meaningful statutory remedies (both damages and injunctive relief), for cloud computing providers and customers

4 Deter Hackers with Meaningful Penalties at National Level

- Promote the adoption of sanctions under national laws that recognize the greater scope of harm when multiple accounts are accessed

¹ <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/>

Protection of Privacy and Data Transfers : EU and International Considerations

For cloud computing services to develop to their full potential, harmonised rules implemented consistently across the EU is essential. The review of the data protection framework provides an opportunity to clarify the rules related to privacy and data protection as concerns cloud computing. Similarly, harmonising the application of EU data retention requirements at Member State level would provide clarity as to whom the directive applies and allow for a single, coherent and cost effective retention period within the single market.

The international dimension of data transfers in cloud computing requires that companies be able to transfer data on a worldwide basis subject to appropriate safeguards for the processing of the data. In order to reduce the bureaucracy and burden on companies transferring data, one possibility could be to streamline and harmonise the notification and approval requirements for Binding Corporate Rules (BCRs) and Model Clauses mechanisms.

European policymakers should also pursue through bilateral or multilateral international dialogue cooperation with regard to minimum protection levels for the privacy and security of transferred data.

Cloud computing providers face multiple, and potentially conflicting, laws within and outside the EU, concerning disclosure of the information they hold. Achieving a better understanding of jurisdictional issues is critical and should be tackled through enhanced dialogue.

Finally, efforts to clarify and extend the coverage of the WTO General Agreement on Trade in Services (GATS) to address online delivery of software and services should continue not only at a multilateral level but in bilateral and possibly plurilateral discussions as well. The efforts should ensure market access, most-favoured-nation (MFN), and national treatment for the delivery of the full range of cloud computing services.

Calls to Action

5 Harmonize Europe's Data Protection Framework at Member State Level

- Clarify the definition of "personal data" across the single market
- Simplify the Data Protection Authority (DPA) notification system with a uniform EU-wide registration form and creation of a common registration database

6 Clarify the Application of Data Retention Rules Across the EU

- Clarify the definition of the services encompassed by an ECS and introduce a single, uniform period for data retention applicable across the EU
- Introduce clarity and consistency on which countries' rules apply with regard to government access and privacy protections (within the EU and at international level)

7 Pursue Bilateral Or Multilateral Cooperation On Protections For The Transfer Of International Data And Assess Existing Mechanisms For The Processing Of International Data Transfers

- Assess the need to reform and streamline the adequacy principle and/or notification and approval requirements for Model Clauses mechanisms and Binding Corporate Rules (BCRs)

8 Clarify Application of Trade Disciplines to the Delivery of Cloud Services

- Extend existing coverage of the GATS with regard to online delivery of software and services to ensure market access, MFN and national treatment for the delivery of cloud computing services

Data Portability and Cloud Interoperability

Data portability and the seamless use of applications that can communicate and interoperate with each other are key considerations for cloud users. The EU has put interoperability at the heart of its Digital Agenda, recognising that the interoperability of services and data is central to promote user acceptance, increased value and choice. Cloud providers must work together to promote the development of market-led standards and ensure that interoperability and portability are addressed in an open and collaborative process.

Importantly, European initiatives relevant to technology standardisation, including the Commissions on going reform of the IT Standardization Framework, should reflect these principles, endorsing technology neutrality and avoiding mandated standards or preferences that will frustrate, rather than promote, interoperability among cloud services and solutions.

Calls to Action

9 Foster Data Portability through Market-led and Technology-Neutral Policies

- Endorse technology neutrality and promote market-led standards development and deployment

Theft of Service and Promoting Respect for Intellectual Property

The cloud is not immune from the perils of software piracy. With cloud technology, it is possible for an individual or enterprise, acting without authorisation from the rights holder, to permit others to access and use software and its functionality. The fact that the making available of software in this way is not authorised may not be apparent to those who access the software. Enforcement authorities should work closely with industry to detect and deter such unauthorised acts, and protect users and their data from unauthorised and potentially unscrupulous providers.

Theft of cloud computing services is another form of software piracy that may occur in the cloud. Traditionally, software piracy generally involves making unauthorised copies of protected works, and

copyright remedies are provided under the Copyright Directive (2011/29/EC) and national copyright laws. Unauthorised use and theft of software functionality delivered in the cloud may not in every case involve unauthorised reproduction of a protected work. In those instances where the provisions of the Copyright Directive are not clearly violated, there may not be clear remedies under existing European law against end users who, without authority, utilize and derive economic benefit from software that is housed in the cloud. Any gaps in existing statutory intellectual property rights should be examined to ensure that right holders have a clear and meaningful framework for protection. A lack of clarity about rights and remedies against theft of services will forestall innovation.

Calls to Action

10 Deter the Theft of Intellectual Property through Cloud Computing Services through Sound Enforcement Policy and Clarity about Rights and Remedies

- Enforce existing law that prohibits intellectual property theft in the cloud context
- Introduce targeted legislation to address unauthorized use of software functionality made available through cloud computing offerings