SCIENCE AND TECHNOLOGY OPTIONS ASSESSMENT
OPTIONS BRIEF No 2014-01, January 2014

Potential and Impacts of Cloud Computing Services and Social Network Sites

About the project

Cloud Computing and Social Network Sites (SNS) are among the most controversially discussed developments in recent years. The opportunities of using powerful computing resources on demand via the web are considered as a possible driver for the growth of the European economy. This project:

- reviewed the latest technological and economic developments,
- identified driving factors and barriers in Europe,
- identified the main actors and their respective interests,
- analysed the impacts on citizens, business (including the IT industry itself) and public administrations, and
- evaluated the effect of a broad range of technical, economic, cultural, legal, regulatory issues and their impacts.

Cloud Computing includes a variety of technical concepts that alter computing infrastructures used by businesses, public administrations and end-users. SNS represent a prominent phenomenon grounding on Cloud Computing with a wide array of services and applications mainly focussed on end-users.

Market and industry perspectives

While the market for SNS already experienced a consolidation, the market for Cloud Computing is still in an early stage, but with considerable growth rates. It is obvious that most of the major players are still of US origin. While the lagging behind might be not as big as sometimes feared, it seems that there are differences in the sophistication of usage between Europe and the US. Overall it can be stated that both technologies are still evolving and that in particular the market for Cloud Computing is still in the flux. Cost savings are considered the most important positive impact for businesses and public administrations, most numbers are based on expectations than on real world experiences though. Flexibility, mobility and innovation as further positive impacts will gain of importance in the mid and long term. Negative impacts are risks for security, dependencies on services and the reliability of services. Regarding the IT industry, Cloud Computing impacts rather the market structure than the industry structure at the moment. However, both enable new services and thereby new business models. Regarding consumers, the main positive impact is convenience; costs are less relevant. Negative impacts are primarily threats to security and privacy. Based on the cost savings and the resulting productivity gains, the creation of new jobs and economic growth are seen as main positive impacts for the society and the economy at large. Recent research shows, however, that productivity gains based on IT do not lead to growth and employment automatically. This requires the presence of certain framework conditions. Negative impacts are loss of technological sovereignty and possibly restrictions of civil liberties. Based on this, challenges were analysed further. Beside technological challenges such as standardisation and interoperability, IT security is challenged.

Privacy and Security challenges

The recent massive surveillances actions and the rise of cyber crime showed the need for a more secure basis of future computing. Cloud Computing as well as SNS challenge the existing data protection regime. However, modernisations such as the new draft regulation need to be continued and filled with life. Since trust is a pivotal success factor the questions of third party access and data retention need to be addressed. The analysis of contractual relations showed that main contractual features like jurisdiction, liability, service levels or acceptable use still raise questions. A similar situation can be found for IT security related issues. Finally the analysis showed the need to address challenges to competitiveness such as vendor lock-in or the lack of fast growing companies as well as challenges in framework conditions like market fragmentation, broadband penetration or skilled people.

Policy options

The project showed that at the moment, there is a unique chance to achieve multiple Cloud Computing and SNS related goals simultaneously. There are no contradictions between assuring European citizens, secure, privacy aware, legally certain and fair use of Cloud Computing and SNS and, on the other hand, in increasing the competitiveness of European ICT industries. Moreover it is possible to exploit the potential of Cloud Computing and SNS to the benefit of both the European economy and society at large. Based on this a coherent and consistent set of options for European policy makers grouped into 4 themes with in total 16 options was derived:

Theme I: Make security a commodity

At the moment ensuring IT security is sometimes difficult. Solutions can be hacked, even if, e.g. a powerful crypto system has been used, or they sometimes they are inconvenient to use for normal users. Therefore it is necessary to support the development of highly secure IT solutions, which are easy to use and which can be adopted by all businesses, both big and small, as well as by all citizens.

- **Policy option 1: Support the development of open and secure software and hardware and encryption methods:** The development of secure open soft- and hardware, which does not contain any backdoors, potential for zero-day exploits, etc., as well as of encryption methods, for instance content or homomorphic encryption, should be explored. For practical usability, it should be compatible with existing software and easy to understand. The latter could be realized using, for instance, virtualization. This should initially be supported by means such as research funding. In addition, the development of these highly secure soft- and hardware could additionally be encouraged, for instance, by (pre-commercial) procurement policies or by making it mandatory in some sectors.
- **Policy option 2: Encourage the use of checklists and security certifications:** To address the day-to-day risks of Cloud Computing, the use of checklists for keeping systems secure could be encouraged, as should the use of sufficient backups, etc.. The use of comprehensive security policies could be certified. Breaches should at least be reported to the certifying institution. In the medium run, certification could show the use of secure computers or secure virtualisation.
- **Policy option 3: Assess the economic viability of large hardware security modules:** To allow confidential processing of data in the Cloud, it could be estimated what such processing in remote tamper-resistant modules would cost when applied on a large scale. This is regarded to be more expensive, but the concrete cost penalty is unknown.
- **Policy option 4: Initiate a dialogue on the structure and governance of the Future Internet:** A high-level dialogue with Internet infrastructure organizations such as ICANN, IANA, IETF and others about the future infrastructure of the Internet and the internationalization of its governance should be established.

Theme II: Establish privacy as a location advantage

For a long time, European data protection standards were seen as a disadvantage for digital business. Recent developments, as well as changing requirements for emerging technologies and a growing digitalization of all spheres, underpin the necessity of modern privacy rules. By modernizing the data protection regime, Europe could not only ensure a better protection of citizens, but also serve as a model for emerging markets, which could be attracted to increase their exchange with Europe. It could underpin this function as a leading example by addressing a fair and secure governance and a structure of an open Internet at a global level.

- **Policy option 5: Proceed with the modernization of data protection:** Support, and if possible expedite, the current process of data protection reform, in particular the clarification of data protection principles relating to cloud computing. This includes the support of the choice of a Regulation as the legal instrument, the strengthening of pre-existing individual rights in the Regulation, the range of new rights offering further control to the data subject (e. g. portability, deletion), as well as the range of novel obligations for the data controller and the accountability principle

- **Policy option 6: Establish the principles of security and privacy by design:** Look further into ways of developing and promoting architectures for Cloud Computing and SNS designed from the beginning to a high level of security as well as privacy by design1 rather than only by trust or legislation.

- Policy Option 7: Support the creation of a European Data Protection Board: Support European level consistency and interpretation mechanisms and the creation of a European Data Protection Board.

- Policy option 8: Ensure the extraterritorial application of European data protection law: Leave the "safe harbour" agreement and explore and implement options to ensure the extraterritorial application of European data protection law as foreseen in the current draft of the regulation.

Theme III: Build a trustworthy environment for digital business and living

Digital life of citizens and business needs legal certainty to ensure new ideas are taken up. Since many emerging technologies in ICT create both new chances and new challenges, there is a need to continually review existing legislation and to adjust it if necessary. Only if people have trust in legal certainty, they will adopt and use new technologies and exploit their potential for the economy and society as a whole.

- Policy option 9: Stipulate the setting of minimum requirements for contracts: Support proposals to stipulate minimum requirements regarding changes to the provisions of contracts, the notification of such changes and remedies for those clients for whom changes are materially significant.

- Policy option 10: Support the standardization of Acceptable Use Policies and Service Level Agreements: Encourage the clarification standardization of Acceptable Use Policies and Service Level Agreements. This includes the support for the development and usage of standardized model clauses and the clarification of the related terminology used in these clauses for both, Service Level Agreements as well as Acceptable Use Policies. It is aimed at preventing providers to misuse their power in particular in relation to consumer or small and medium sized enterprises.

- **Policy option 11: Eliminate jurisdictional uncertainty:** Consider support for proposals that address issues relating to jurisdictional uncertainty. This may include supporting initiatives to stipulate compliance with EU law, minimum requirements regarding the disclosures to a third country and obligatory use of Mutual Legal Assistance Treaties.

- Policy option 12: Support the development of Cloud specific certifications: Support proposals for the development of EU Cloud-specific certification, which are meaningful, e.g. in regard to privacy contains automatic information of DPA in case of any access by others. Promote their use through the adoption by public sector organizations within the EU.

Theme IV: Create an inspiring ecosystem for ICT industries

A crucial precondition for a competitive ICT industry is an inspiring ecosystem. This is illustrated by examples in other regions or other industries. Such ecosystems contain many components. Of particular importance is support for innovative and fast growing companies as well as the provision of sufficient framework conditions.

- Policy option 13: Encourage the creation of European market players: Support the creation of new disruptive developments in technology and business models such as really secure platforms for mobile devices or businesses exploiting the potentials of the Cloud and SNS ecosystem.

- Policy option 14: Support standardization and interoperability: Support the efforts for standardization and interoperability in Cloud Computing and SNS solutions. This aimed at enabling user to exploit the full potential of a vivid and competitive European market. It is also aimed at preventing the misuse of market power for setting de facto or corrupted standards for example in the fields of data portability or encryption. Possible ways to achieve this could the adoption of standards or interoperability frameworks in public services or strengthening of the role of European bodies like ENISA or ETSI.

- Policy option 15: Empower people across all strata of society: Empower people by supporting the appropriate education of a sufficient number of people, users as well as developers. The first refers to both technological knowledge and to knowledge as to the potentials and risks of emerging technologies such as

[1] "Privacy by design" could mean to use, e.g. pseudonyms of attribute-based credentials (showing e.g. that somebody is of a certain age).

Cloud Computing and SNS. The latter refers to the support of the integration of groups less represented in the ICT and related industries such as women, elderly people or people with less formal education.

- Policy option 16: Reconsider current broadband strategies: Review the progress and methods of the different EU member states and elsewhere. Possible examples are Sweden or Japan. Based on this identify and adopt best practices. This includes addressing the problems of financing infrastructures ensuring an appropriate balance of interests for all stakeholders. Furthermore, increased competition between fixed, licensed and unlicensed communications would be supportive.

Based on a STOA study by the same title published in January 2014 (PE 513.546).

Editors:
Fraunhofer Institute for Systems and Innovation Research (ISI), Karlsruhe (project co-ordinator); together with the Institute of Technology Assessment (ITA), Vienna; the Institute for Technology Assessment and Systems Analysis (ITAS), Karlsruhe; and the Danish Board of Technology (DBT), Copenhagen, as members of ETAG.

Authors:
Dr Timo Leimbach, Mr Dara Hallinan, Dr Daniel Bachlechner (Fraunhofer ISI)
Dr Arnd Weber, Mrs Maggie Jaglo, Dr Leonhard Hennen (ITAS)
Mr Rasmus Øjvind Nielsen (DBT)
Dr Michael Nentwich, Mr Stefan Strauß (ITA)
Dr Theo Lynn, Mr Graham Hunt (DCU/IC4)

The opinions expressed in this document are the sole responsibility of the authors and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

For further information, please contact:
Peter Ide Kostic, STOA Unit
Directorate for Impact Assessment and European Added Value
Directorate-General for Parliamentary Research Services
European Parliament
Rue Wiertz 60 - RMD 00J0016, B-1047 Brussels
E-mail: stoa@europarl.europa.ep

www.europarl.europa.eu/stoa/