

# Openforum Academy

## Report

### The Cloud Computing Workshop

---

**Date:**

*1<sup>st</sup> March 2012*

**Venue:**

*Google Offices. Brussels, Belgium*

*Organized by:*



## Cloud Computing Workshop Report

### **Disclaimer**

*This report is prepared by the rapporteur, Dr. E. Altsitsiadis, for Open Forum Academy (OFA) in support of the Cloud Computing Workshop. The summaries of the speaker presentations and panel discussions in this report are based on the rapporteur's notes and they are not in any way binding or necessarily complete. No electronic means were used in recording the actual speeches. All effort has been given to reflect and convey objectively the essence of the speakers' presentations and the discussion. The views expressed in the report do not necessarily reflect those of the rapporteur, the workshop organizers or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.*

---

### *Summary*

The workshop brought together high-level experts to discuss three broad aspects of cloud computing; the economic impact, the legal aspects and the way to move forward. The economic opportunity is irrefutable - If you live in a multi-device world, you simply need the cloud. The cloud will have a significant impact on our entire economy; from the micro level and the numerous benefits it brings to supply and demand alike, to the positive macro-effects in new job creation and GDP contribution. There are serious obstacles though in claiming these benefits, from practical operational limitations to misconceptions, distrust and a legal framework that is largely fragmented and complicated. The speakers broadened our understanding of these weak points, downplaying some issues that are overly considered important, while pointing out others that are crucial, yet evade our attention. The workshop illustrated that there are a lot of misconceptions but also a lot of common ground and it is becoming apparent that the way forward passes through better communication and collaboration, whether at the level of EU-US governments, Industry-Policymakers or Providers-Users.

*“The cloud will happen; the question is whether it will happen to us, with us, or by us“*

### *Speakers*

#### Welcome

Prof. Peggy Valcke, KU Leuven

#### Keynote address

Prof. Paul Schwartz, *University of California, Berkeley*

#### Panel 1: The Economic impact of the Cloud

Prof. Federico Etro, *University of Venice, Ca' Foscari*

Dr. Andreas Tegge, *VP Government Relations SAP*

Jonathan Sage, *IBM Governmental Programmes*

Hans Graux, *KU Leuven, timelex*

#### Panel 2: Legal aspects of the Cloud

Chris Kuner, *Partner, Hunton & Williams*

Jaap van Oss, *EUROPOL Cyber Crime Centre*

Kenneth Propp, *Legal Counselor, US Mission to EU*

Prof. Giuseppe Vaciago, *Cybercrime Research Institute*

#### Panel 3: The Cloud: The way Forward

Dr. Carl-Christian Buhr, *Member of Cabinet of Commissioner Neelie Kroes*

Silvia-Adriana ȚICĂU, *European Parliament*

Dr. Marnix Dekker, *ENISA, Application Security Officer*

Marc Crandall, *Senior Manager of Global Compliance, Enterprise, Google*

#### Closing remarks

Paul Hofheinz, president and cofounder of the Lisbon Council

**Moderator:** Paul Hofheinz, president and cofounder of the Lisbon Council

**Rapporteur:** Dr. Efthymios Altsitsiadis, *Research Group Marketing, KU Leuven*

#### **Acknowledgements**

Special thanks to Patricia Wruuck, Google, for her timely communication and support and to Dr. Eleni Kosta, KU Leuven, for her valuable contribution.

### *Welcome speech – Prof. Peggy Valcke*

**Prof. Peggy Valcke** welcomed the participants and briefly outlined cloud computing, from its roots back in the 50s until today's explosive growth. Prof. Valcke highlighted the European Commission's determination to develop a robust EU-wide strategy on cloud computing that could help boosting Europe's digital economy. Yet, she mentioned the strong concerns about the overly prescriptive rules in the recent EC's proposal for a Data Protection Regulation, which according to the Business Software Alliance (BSA) could undermine the economic advantages that a truly global cloud can provide.

Quoting BSA's report<sup>1</sup> and the cloud policy blueprint, she pointed out that in order to obtain the benefits of the cloud, policy makers must provide a legal and regulatory framework that promotes innovation, provides incentives and promotes confidence that the cloud will deliver the benefits without sacrificing expectations of privacy, security and safety. Prof. Valcke stressed that although this sounds nice and simple, implementation in practice is a lot more challenging, as we should not sacrifice privacy, security and safety in view of cloud computing implementations, and expressed her ambition that the workshop will be a useful exploration along these lines.

### *Keynote Address – Prof. Paul Schwartz*

#### *Privacy developments in the USA*

**Prof. Schwartz** started his keynote speech by briefly analyzing the recent privacy developments in the USA, strongly emphasizing their importance. On March 2011 the Obama administration announced support for "baseline privacy law", while on February 2012, announced and outlined a set of seven basic Online Privacy principles. The overall aim is to create a baseline for privacy law and cover areas that are not yet covered. California Attorney General announced a settlement that establishes privacy policies for apps. The owner of an online site is obliged to have and post a privacy policy for that site, but now companies have agreed to extend this requirement also for apps. Web firms have recently agreed on the "Do Not Track" button, a notion inspired by the successful "Do Not Call List" initiative. Finally, 2011 saw a number of important F.T.C. settlements (Facebook, Google Buzz).

#### *Benefits of the cloud*

The second section of the talk focused on the economic benefits of the cloud. Prof. Schwartz referred to Ronald Coase's "make or buy" question. Cloud computing brings a new answer to the question of whether a company should internalize parts of its operations, pointing out the importance of saving transaction costs. Firms today want to stay lean, small and concentrate on what they do best. Cloud computing locates computing resources on the Internet to make them highly dynamic and scalable. It offers different functions and operations packaged as modular units and as a result offers amazing flexibility as to when relationships should be structured internally or externally. Furthermore, the cloud offers dramatic flexibility and scalability in processing capability; cloud users no longer need to own technology, whether hardware or software. The cloud market will continue to grow; the mobile web will outgrow the personal computer and as Prof. Schwartz quoted "if you live in a multi-device world, you simply need the cloud."

#### *European developments*

European developments have a lot to do with trust and the fact that clouds are run by US companies. European customers are getting worried that the US government is getting access to too much data and as a result US companies report problems with their EU customers. There are currently two manifestations of this EU distress; a proposal about the French cloud and the German cloud. Both these ideas reflect this growing concern about US access

---

<sup>1</sup> <http://portal.bsa.org/cloudscorecard2012/>

on French and German enterprise and government data. The US on the other side is wondering whether there is a debate about the German cloud and data retention. Following a different dimension, the EU announced on January 2012 the European Cloud partnership, which intends to make Europe more cloud active.

#### *Legal treatment of the cloud in the USA*

The US approach to information privacy law is characterized by complexity. There is a lack of omnibus privacy law but the US has sectoral regulation. There is a weak constitutional right to privacy and one that applies only when “state action” exists, but not against actions carried out by private entities. Some states have strong sectoral regulations. Some tort laws ensure also protection to privacy; for example the right to privacy in tort law exists in California. Although there are no data protection authorities, equivalent to the European model, the US has a strong presence of non-government associations that form an integral part of the scenery, such as FTC, state attorney generals or advocacy organizations.

The PATRIOT Act is often a cause for mistrust; Prof. Schwartz acknowledges its emblematic nature, but questions whether it is really a problem. Although the PATRIOT act is commonly mentioned in relation to the regulation of the US cloud, the PATRIOT Act is not really about cloud and vice versa. Nevertheless, and in more relevance to the cloud, the US does not have strong constitutional rights applicable to the cloud, especially as regards the third party doctrine. For instance, in relation to the protection of personal information, when an entity gives data about a citizen to a third party, then the government can get access to this information without much difficulty. The Electronic Communications Privacy Act (ECPA) is really complicated - written from a viewpoint of technology of 1986; companies face difficulties in knowing what applies to which categories of data. Under ECPA data in storage for more than 180 days are less protected. Finally Prof. Schwartz downplayed the impact of the National Security Letters, as the FBI now needs to obtain a court order before issuing such letters for investigations and for transparency reasons it should communicate information on how many of them are issued in a year.

#### *Moving ahead*

The Digital Due Process Alliance, a coalition formed by the majority of major companies and organizations, has asked for the reform of ECPA, requiring a general search warrant based on probable cause. Such actions have been successful in the past. More transparency is needed: The ratings of the Electronic Frontier Foundation (EFF) evaluating companies for their transparency and efforts to support user privacy can contribute to motivating company decision makers and influence their decisions towards more transparency. There is a need for more gov-2-gov work. The US President calls for a global consensus for emerging privacy issues as it becomes clear that we need robust collaboration worldwide to solve trust issues. However, it is difficult to reach an agreement among the various states even within the US, as they have different laws and ensure different levels of protection. Prof. Schwartz believes that there will not be a new law regulating legal issues on the cloud, but maybe amendments to existing legislation will take place.

#### *Discussion and conclusions from the keynote-speech*

Some of the questions and remarks focused on the premise of the European mistrust. When asked to think of ways to solve the fact that companies fall victims of jurisdiction, Prof. Schwartz did not consider the French and German Cloud ideas as potential solutions, as assets in the US will remain under pressure. A participant noted the contradiction between competing on the one hand and sharing resources on the other, and whether the cloud will eventually be just a utility in the future. Prof. Schwartz used an example to stress the likely fact that companies will move out of the cloud as IBM did once it realized the utilization of the personal computer industry.

Replying to a question, he stated that it is difficult to predict success of the new legislation developments, and he stressed that companies that already have a privacy policy established would like to have a baseline law for privacy, while the preemption problem about federal Vs State legislation continues to exist. The response to the question

whether we need laws on the internet, he mentioned that our perspective changes the nature of harms and benefits, and although there won't be a law for the cloud, if new problems arise there will be a need for new categories.

In his conclusion, Prof. Schwartz highlighted the real value of data analytics. He summarized the difference in EU-US perspectives: the EU does not start from an innovation goal but from the right to privacy. The right thing would be to find the right way forward, and a good first idea would be to identify and study how much difference there is about intelligence, agency and law enforcement among the US and EU but also among Member states.

### *Panel 1: The economic impact of the cloud*

#### *Speaker Summaries*

**Prof. Etro** talked about the impact of the cloud in the entire European economy. The switch from fixed costs to operating costs has macroeconomic effects on the whole economy. For the public sector the cloud brings efficiencies in healthcare, education and e-government, while in the private sector the cloud will result to cost reduction at various levels and to higher productivity.

In his study<sup>2</sup>, the conservative scenario forecasted a strong impact of cloud computing on job creation and significant impact on employment and GDP growth. Prof. Etro downplayed the negative impact of the cloud on job creation; for every traditional IT jobs lost he estimates about eight new ones across the economy to be created.

Based on other case studies, he suggests that a 10-35% is a rational estimation for cost reduction from the adoption of cloud computing in the public sector, somewhat less of the cost reduction expected for the private sector. Prof. Etro suggests that cloud computing in the public sector should be promoted to signal adoption in the private sector, also through subsidization of adoption.

**Dr. Tegge** talked about how Europe can assume a leading role in the cloud. He urges to focus on the broader issues and to extend the focus on the industrial partners. Contrary to earlier belief, the macroeconomic benefits of the cloud are significant; the cloud can be a real driver for the economy, and this realization is important. Infrastructure, where US currently leads, will fast become a low margin commodity market, while platform development and applications and content, areas in which EU firms are very relevant, will grow. EU firms' flexibility in partnering and trustworthiness should be used to gain advantage.

Dr. Tegge identifies four steps crucial for Europe to lead. Cost reduction is not everything, there are networking benefits. In the future, companies will collaborate in business cloud communities and *we need to understand the cloud as an ecosystem* and adapt to the resulting changes. Then we need to *understand the key positions of "centers of gravity" in the network*; the centers of the cloud will define all the important aspects and nurture the other players within the ecosystem. The smaller players are an integral part of the ecosystem and we need their innovation capacity to *leverage the potential of biodiversity*. Finally we need to provide a trustful and harmonized *premium legal and regulatory environment*, without red tape but with high standards of privacy. A global golden standard that incorporates current standards, supports all business models and deals with all issues, including customer compliance is the difficult, yet rewarding way forward.

**Mr. Sage** talked about the economics of the cloud. Everyone will be using the cloud as traditional IT has changed forever through the ability to utilize huge infrastructure and the revolution in how people use the cloud. The smart-

---

<sup>2</sup> 2009, The economic impact of cloud computing on business creation, employment and output in Europe, Review of Business and Economics

phone explosion will render the PC another piece of junk we can get rid of. His answer to the “make or buy” question is that we will have to buy.

He stressed that the EU competitiveness issue has more to do with the lack of venture capital than it has to do with more regulation; you cannot regulate innovation. The EU internet, like the EU search engine, will not work; it is a global business. The economic benefits of the cloud will disappear once more EU specificities are introduced. Overregulation or local initiatives are likely to reduce the impact – what is needed is a global model. Mr. Sage explained the different business models in play, along an “On-Off Premise” axis and analyzed an array of possibilities (including hybrid models), highlighting that transition from old to new might not be always easy.

Talking about the market, he stressed that security is a top concern with regards to the actual transition to the cloud. However, it is often used as an excuse for not moving forward. The cloud is about new business value, it is a catalyst for change that allows companies to rethink IT and the way they do business.

**Mr. Graux** delivered his speech on cloud economics from an SME perspective. He downplayed the importance for SMEs of the US based servers issue; in reality a conflict will be a problem in Ireland as much as in the US. Data protection, however, is an important issue that results in costly complexities. SMEs have to ‘buy’ they cannot afford to ‘make’ solutions. Most of the times SMEs do not have a dedicated tech team, they don’t have the power to negotiate unique concerns with providers. For SMEs the change from the cloud is not that big; they still had to buy solutions before, now they just need to buy cloud solutions.

Weighing the pros and cons of cloud computing, Mr. Graux found the gains in terms of legal compliance to be neutral. In terms of security, service cost and usability, however, there are moderate advantages for SMEs; cloud reduces security costs and offers simplicity functionality that would otherwise be unavailable. The biggest benefits are related to reliability, where the cloud minimizes risks. Overall the cloud offers ‘a bit more value for money’ but there is not enough customization, support and communication for SME customers. The economics make sense but adoption will increase through improved transparency and compliance.

### *Panel 1 Discussion and conclusions*

A question was raised regarding transparency and compliance. The speakers suggested that audits and SLAs will not suffice, but the fact that there were absolutely no answers on the issue a few years ago, is indicative of the growing maturity. In the future auditing rights will be guaranteed by the service providers. Customers will put pressure on service providers and this will be beneficial for all. EU policy should clarify what the service providers must do.

Another question referred to the selection of standards, which in many cases can be competing. The speakers agreed that selection is market driven; standards recognized are more trusted by customers and are preferable. Multiple standards are a problem that companies need to cope with, as customers ask for compliance with different standards. In another topic, it was suggested that it is better to agree on standards on processes rather than standards on specific technologies.

The speakers concluded that there is still excessive complexity for the customer and more standardization should be made accessible to the end user. Policy makers can play an important role; fiscal motives can be effective. Standards are already there, and there is a trend for ISO and ITU coherence at a global level.



*Panel 2: Legal aspects of the cloud**Speaker Summaries*

**Mr. Kuner** started the discussion on the legal aspects of the cloud suggesting that thinking of the cloud is comparable to thinking of the internet. In this respect, cloud legal aspects are pretty much internet issues. Parts of the legal aspects are over-hyped, another part, however, remains important. From a business perspective, territory seems to be of lesser importance; the cloud is less territorial and it now brings up new issues that existed but were not as visible. Private law instruments could be a mean to address these issues.

As Mr. Kuner stresses, there has not been considerable attention to the lack of territorial connections among cloud and users and there was a lack of sophistication with regard to contracting of cloud services. Public law issues in cloud computing are less easily solvable and new jurisdiction and applicable law still need a national law as basis. Many of these issues can be attributed to a lack of political agreement but they cannot be considered only an internet or cloud issue. A lot of the problems stem from the fundamental difficulties governments to agree on basic issues. Companies are the actual explorers, reaping the benefits but also paying the price of been caught among governments. These problems if not solved, will eventually cause real problems on e-commerce.

**Mr. Van Oss** delivered his speech from the perspective of a law enforcer. He considers the cloud to still be a fuzzy concept, for which is often difficult to find answers. Mr. Van Oss gave an example of self-regulation in the cloud where a gang was outed by Facebook and the user community rather than being arrested. Cyber-criminals use the internet as infrastructure for their attacks. This infrastructure is built over four phases and is based on their own cloud. Cyber criminals have to work together in non-hierarchical market oriented groups – it is no longer a matter of the lonely hacker. Mr. Van Oss suggests that they might be even more efficient if they start using cloud services to build a more reliable base for their operations.

In his remarks on law enforcement methods he mentioned that ‘Following the money’ is not always a successful method to tackle cyber-crime. There is a risk of running the investigations in isolation. The result will improve once the money trail is combined with malware investigations and an information position on the Underground Economy. The information necessary for law enforcers to do their job is out there, but they need help from other partners. There are important challenges ahead; instead of hacking computers the criminals can hack the cloud. They can use the cloud not only to get data, but also to perform other parts of their business. We need to rethink instruments and investigation methods to adapt to the cloud, and in this effort we need joint actions with all stakeholders and clients.

**Mr Propp** talked about cloud computing and law enforcement access to data on the cloud. Existing methods are under pressure from the changes brought by the cloud. The US has signed numerous agreements with the EU in law enforcement and has managed to build a legal framework. Information sharing needs though have increased.

Mr Propp stressed the misconception that the EU cares more and is more successful in protecting personal data. The US-EU high-level contact group set to tackle such misconceptions made progress in defining common principles, which suggests that there are commonalities between the EU and US. Mr Propp referred to the belief that US protects less foreign people’s data as another misconception, based on the US Privacy Act. He concurred that the Privacy Act is merely a piece of the puzzle; there are other laws that do protect these data. He highlighted that the cloud does not change the legal construct, but it does put stress on it. He further addressed another misconception that the PATRIOT Act has changed everything regarding access to electronic communication. Mr. Propp noted that it did broaden the authority of the FBI to retrieve data through national security letters, but downplayed their importance. Mr. Propp argued that the US system in this area is in fact more transparent than the European.

**Prof. Vaciago** introduced his topic by presenting statistics on terrorism and emphasized the importance of cybercrime. He briefly discussed the PATRIOT act and stressed that it has been copied in many countries, including countries that

have criticized it harshly, like Canada. In Europe several cloud providers offered Patriot-Act-free services sheltering their users from US control. European Commissioner Reading said on the subject that although she encourages cloud computing centers in Europe, she thinks that we need free flow of data between the two continents. According to Prof. Vaciago, what we need is jurisdictional principles. However, it is difficult to apply the territorial principle, while the flag principle is impractical. The power of disposal approach could solve the jurisdiction problem; courts can be ignorant of the technical aspects. Interestingly, the EU is asking for more data than the US does. Overall no clear solution on the jurisdiction issue currently exists.

In his conclusions, he argued that the big issue is the loss of data location because of the cloud which makes the job of the investigator comparable to that of a puzzle. The digital due process is a needed step for the review of the complicated ECPA. What is also crucial is the EU-US collaboration. The real fear is not the PATRIOT act; face recognition together with increasing public disclosure and electronic surveillance enables geo-locating, raising new issues in data protection.

### *Panel 2 Discussion and conclusions*

A question was raised as to why not more research is taking place. Indeed the speakers consider that the need is overlooked and that objective 'hard' research is needed that is not too "political" oriented. In the question whether we need separate laws for the internet the speakers replied that we need a new approach to address the cloud area, not necessarily new laws; it is more important to focus on processes. If we want to fight cybercrime we should think of new ways and use the tools available. There's no big difference among online and offline crime and we should help the law enforcers.

One participant asked whether the national legislation is enough. It is indeed a problem of localization; one solution would be to use agreements, terms and conditions and so on. There is a need for better ways to get agreement online, as long texts are not efficient. On a second layer, government agreements are required as even the most complicated issues can be solved if there is a governmental basis. There is a need for government agreements, but it is increasingly difficult to get to the root of the problem instead of using "band aids".

In their concluding remarks, the speakers suggested that we need to work on getting governments more involved in talking to each other more; industry and civilians should hold them to the task. Cloud computing caused the explosion of jurisdiction problems. In some areas progressive solutions that could provide a basis for more difficult issues exist, yet it is still too early to assess them. At the moment there is a need for new ways to fight cybercrime; technology should help the law.

### *Panel 3: The cloud - The way forward*

#### *Speaker Summaries*

**Dr. Buhr** presented European Commission Vice-President Kroes's plans to present, before summer 2012, a European Cloud Computing Strategy. The Strategy will be a combination of a horizontal analysis of the various policy areas impacting on, or being impacted by, cloud computing, as well as an action plan to address any barriers to better cloud offerings and deployment. He referred to a number of recent speeches in which the Commissioner had announced the strategy and had explained various building blocks, e.g. the role of the newly proposed legal framework for data protection in the European Union, the impact of cloud computing on online content businesses and her goal to harness the large public ICT procurement budgets across the EU to improve market conditions. In his conclusion, Dr. Buhr stressed that 'the cloud will happen; the question is will it happen to us, with us or by us...

**Ms. Ticău** referred in the beginning of her speech to the initiative report on "A Competitive digital single market - eGovernment as a spearhead" and outlined the benefits that stem from the cloud mentioning also the advantages for the cross border market. She then called for better involvement of local and national level. It is useful for SMEs that

they have access to public information but there are some crucial issues. It is important that emphasis is placed in order to respect the rights.

The European Cloud Partnership should not be only public, but ensure private sector participation. Interoperability and standardization need to be promoted as it is crucial for SMEs, and data ownership issues must be addressed. A European model for Service Level Agreements would be useful, provided that it offers simplicity. Ms. Ticău then stressed the importance of financial resources; there are not enough sizable investments and the public sector can play a role to boost cloud adoption. In conclusion, the European Parliament will support the cloud computing strategy but it also calls for an action plan, with clear actions, financing and motives.

**Dr. Decker** spoke about security and data breaches. Talking about the rising trend of information security risks over time, it can be argued that there is a different approach between old and new technologies; the latter are associated with bigger risks. Dr. Decker presented their approach and presented statistics on Zeus, a 2007 Trojan, that suggest that the majority of the infected systems had up-2-date antivirus security. He further argued that hacking groups releasing information in public are not the biggest problem, hackers that don't are.

According to Dr. Decker, cloud computing, smart-phones and social media are part of the solution. Even though there are important concerns - security is costly, social media face serious trust issues, smart-phone apps can be used to spread malware – these technologies are the way forward. He focused on two data breach statistics: 92% of attacks were easy while in 86% of the cases the victim was clueless as the breach was discovered by third parties.

In practice policy makers assume that security issues have to be addressed otherwise customers will leave; this belief is rather weakened, however, as despite the many large data breaches, customers keep on putting data online. Importantly, there are serious weaknesses in detection; the majority of attacks go undetected, while most of those detected are not reported and they are swept under the rug.

Dr. Decker discussed a number of cloud specific benefits. He referred to the elastic resources and the leverage; security is expensive and the scale helps purchasing otherwise expensive security, both in terms of software but also in terms of cost of specialists. The cloud offers remarkable service resilience where local systems would fail (e.g. the recent Japan tragedy), but there are risks in sharing resources that are not well isolated. In his conclusion he stated that security is a driver for cloud computing and argued for a bottom-up approach focusing on procurement.

**Mr. Crandall** stressed the importance of cloud computing and by extension of the European data protection developments for Google. He praised the importance of the European Cloud partnership, but noted that from a global perspective it is difficult for customers to comply with the EU legislation. People should not be stuck in one service; as also stressed in Google's data liberation front, customers that want to leave a service should be able to do this, despite the difficulties. Mr. Crandall commented on the inconsistent security jurisdiction and the way to cope with different security standards, stating the need for common standards – praising the work of ENISA on the topic.

There is a balance that should be sought between standardizing requirements and the regulatory environment that deals with challenges. If everything is too homogenous, the legislator will be unable to protect his own citizens. When a cloud provider has to mediate among Member states and the EU it is very difficult. Google has large numbers of users and if 1% of them used the right to audit, it would have significant practical operational implications. It is therefore critical for cloud providers to explain efficiently to regulators that security concerns are important, but so are the operational aspects of security. In his conclusion, he stressed the need for prompt action and that is why Google fully supports Vice President's Kroes work.

### *Panel 3 Discussion and conclusions*

A question about whether legislation should be developed focusing on processes or on technology was raised. The speakers suggested that putting technical parts in legislation will make it impossible to keep up with progress and therefore a higher level approach is better. Nevertheless, if certain technical aspects are not specified in the legislation it would not be efficient either. The key is to find the right balance between legislative provisions and technical details in order to have some technological aspects but not to exaggerate as to let the market evolve. From the view of the European Parliament, the reluctance with regards to the delegated acts proposed by the EC was expressed, along with the need to limit the mandate of the EC. A participant made a remark that reporting data breach is a first step and asked whether it is efficient. The speakers replied that the new telecom package has provisions for data breaches; the European Parliament strengthened the mandate of ENISA.

In their conclusions the speakers stressed that Europe is not alone – we should think and see globally and just find the way forward together. A lot of issues can be solved with engaging regulators and presenting them the operational reality. A bad law could be a failure to understand and this is fault can be attributed to the private sector for not communicating the operational reality to the legislator.

### *Closing remarks*

**Mr. Hofheinz**, the workshop's moderator, briefly summarized the discussions by stressing the key points. The economic opportunity of the cloud is irrefutable; the cloud will have an economic impact. The existing legal framework though is fragmented and characterized by uncertainty. Ignorance leads to more uncertainty and this is prohibiting understanding among the US and the EU, making it obvious that we need better communication. Quoting Dr. Buhr, he concluded that the cloud will happen, the question is will it happen to us, with us or by us.



## Speaker Bios

### **Prof. Peggy Valcke**

Prof. Dr. Peggy Valcke is a leading European expert on media and communications law. She is a full time research professor at the Katholieke Universiteit Leuven, teaches media law at the H.U.Brussel, is visiting professor at the University of Tilburg and lectures in the Florence School of Regulation (European University Institute). She is the current director of the Interdisciplinary Centre for Law & ICT (ICRI), a research centre at the Faculty of Law of K.U.Leuven, specialized in legal aspects of the information society and one of the founding partners of the Interdisciplinary Institute for BroadBand Technology (IBBT). In 2006, she was visiting professor at Central European University in Budapest, Hungary, and lecturer in the Oxford/Annenberg Summer School. She is a member of the General Chamber in the Flemish Media Regulator and of the Belgian Competition Council.

She is a frequently invited speaker at conferences and expert workshops and has published widely in international journals (in English, French, German and Dutch) on a broad range of topics related to electronic communications law, media law and competition law. Besides being the editor of the International Encyclopedia of Media Law, she is also a member of the editorial board of several journals including The Journal of Media Law; Computer, Law and Security Review; Journal of Information Policy; and e-Competitions."

### **Paul Schwartz**

Paul Schwartz is a leading international expert on information privacy law. He is a professor at Berkeley Law School and a Director of the Berkeley Center for Law and Technology. Schwartz has testified before Congress and served as an advisor to the Commission of the European Union and other international organizations. He is a frequent speaker at technology conferences and corporate events in the United States and abroad.

Schwartz is the author of many books, including the leading casebook, *Information Privacy Law* and the distilled guide, *Privacy Law Fundamentals*, each with Daniel Solove. His over fifty articles have appeared in journals such as the Harvard Law Review, Yale Law Journal, Stanford Law Review, and Chicago Law Review. Fluent in German, he contributes to German legal reviews.

Schwartz is a past recipient of the Berlin Prize Fellowship at the American Academy in Berlin and a Research Fellowship at the German Marshal Fund in Brussels. Schwartz is also a recipient of grants from the Alexander von Humboldt Foundation, Fulbright Foundation, the German Academic Exchange, and the Harry Frank Guggenheim Foundation. He is a member of the organizing committee of the Privacy Law Salon and of the American Law Institute.

### **Federico Etro**

Federico Etro is Professor of Economics at the University of Venice, Ca' Foscari. He is an expert of industrial organization with publications on American Economic Review, International Economic Review, European Economic Review, Economic Journal and leading applied works on the economics of cloud computing, online advertising, and antitrust policy for the New Economy. He studied at the Catholic University of Milan and the University of California, Los Angeles, has taught at the University of Edinburgh, the University of Milan and Luiss in Rome, and has been research assistant for the National Bureau of Economic Research in Boston. Etro's main research is focused on understanding what shapes the structure of markets and the role of market leaders in these markets. The essay Innovation by Leaders (2004, Economic Journal) was popularized by the magazine Economist (Slackers or pace-setters?) as a solution to the Arrow's paradox on the incentives to innovate of dominant firms. The first general characterization of the equilibrium behavior of leaders in industries with open entry was developed in Aggressive Leaders (2006, Rand Journal of Economics) and Stackelberg Competition with Endogenous Entry (2008, Economic Journal). The approach developed by Etro for the analysis of markets, the Endogenous Market Structure approach, has been presented in different international lectures, including the Bi-annual Lecture of the Catholic University of Leuven (2007) and

the Dynamic Competition Lecture of Osaka (2009). Etro wrote two books for Springer, *Competition, Innovation, and Antitrust* (2007) and *Endogenous Market Structures and the Macroeconomy* (2009) and co-edited for Oxford University Press a volume on *Competition Law and the Enforcement of Art. 102* (2011). He also writes editorials for the Italian newspaper *Il Giornale*, and has written columns for *Vox* and multiple international newspapers.

### **Andreas Tegge**

Dr. Andreas Tegge is Vice President for EU Government Relations at SAP and heads up SAP's EU Representation Office in Brussels. In this capacity he is responsible for managing all relations of SAP with the European Commission, the European Parliament and the Council. He also represents SAP in various European Trade Associations and policy platforms such as Digital Europe, the European Internet Foundation, the Business Software Alliance, the European Software Alliance, the Alliance for European Logistics, the Transatlantic Policy Network and the American European Community Association.

Within Digital Europe he is Chairman of the Digital Economy Policy Group and Chairman of the eGovernment Issue Group. Andreas is also a Member of the Executive Board of the European Internet Foundation, the European American Business Community and the Executive Committee of the European Software Alliance. He serves as the rapporteur of the Digital Economy Working Group of the European Ideas Network.

In his previous career at Deutsche Telekom (1991-2005), Andreas had held various senior positions: From 2001 until 2005 he served as Senior Vice President for EU Government Affairs, based in Brussels. From 1997 until 2001 Andreas headed Deutsche Telekom's Government Affairs office in Washington, DC.

Andreas Tegge studied at the Universities of Göttingen, Germany and the University of California in San Diego, USA. He received an MA in Social Science and a PhD in Economics at the University of Göttingen, Germany.

He has published various academic papers on ICT policy issues and is the author of a book on the International Telecommunications Union (ITU).

### **Jonathan Sage**

Jonathan is a member of the global technology policy team within IBM's Governmental Programmes. He is the technology policy lead for the EU with special focus on competition policy, intellectual property policy and standards. He is responsible for relationships with European Institutions and EU member states and represents IBM in several industry associations in Brussels covering technology policy. Prior to taking on this role, Jonathan was a managing consultant in the IBM's Strategic Change consulting practice in the public sector based in Belgium. Before joining PricewaterhouseCoopers where he led the EMEA internal knowledge management team, and then IBM, Jonathan was marketing director for a UK software company which pioneered the first eCommerce applications. He also spent 6 years as Commercial Attache for the British Embassy in Vienna responsible for trade relations in the capital goods sector. During this period he held a part time post Assistant Professor at the University of Business Administration and Economics in Vienna. He was also on the faculty of the Open University Business School for its MBA course and tutor in Strategy for Austria and the Czech / Slovak Republics. He also worked earlier in his career at the United Nations in Vienna (UNIDO and IAEA) in human resources. Jonathan holds a degree in modern languages from the University of Oxford (MA) and an MBA from Henley Business School, UK.

### **Hans Graux**

Hans Graux is an ICT lawyer and founding partner at the law firm *time.lex* ([www.timelex.eu](http://www.timelex.eu)), a Brussels based boutique firm specialised in ICT law and ICT policy making. In addition, he is academically active as an associate researcher at the Interdisciplinary Centre for Law and ICT

([www.icri.be](http://www.icri.be)) at the University of Leuven. With his mixed legal and technical background, he frequently assists the European Commission and private sector clients in determining legal requirements for the implementation of innovative ICT projects or policies across multiple Member States. As such, his recent work has focused a lot on cloud computing, including specifically data protection and compliance challenges. One of his recent studies for the European Commission specifically examined the security, privacy and trust challenges to be overcome in cloud computing.

### **Chris Kuner**

Christopher Kuner is a partner in the Brussels office of the international law firm Hunton & Williams. Mr Kuner is Chairman of the International Chamber of Commerce (ICC) Task Force on Privacy and Data Protection, and participates on behalf of the ICC in the work of other international organizations such as the Council of Europe and the United Nations Commission on International Trade Law (UNCITRAL).

Mr Kuner has served as a consultant to the Organization for Economic Cooperation and Development (OECD) on data protection issues, and is a visiting lecturer in data protection law at the Vienna (Austria) University of Economics and Business Administration. Mr Kuner is author of over two dozen articles in English and German on legal topics, as well as several books, including most recently the book 'European Data Protection Law: Corporate Compliance and Regulation' (Oxford University Press 2007).

His work at OII centres on conducting research for a major scholarly article on the private international law aspects of privacy and data protection on the Internet, and in particular, which privacy or data protection law should apply to online activities under European law, and which courts should have jurisdiction over such activities.

### **Jaap van Oss**

Jaap van Oss is currently working as a First Officer in the Europol Cyber Crime Centre. His main responsibility is leading the operational activities of Europol in this area. Core of that work is AWF Cyborg, Europol's project to tackle serious and organised cybercriminals affecting Europe and beyond.

Jaap van started in the Dutch National Crime Squad years ago, 1996 to be accurate, and has been active in fighting cybercrime ever since. During that time he was involved in different Cybercrime projects for the Dutch National Police, such as the "Cybercop" and "Digital blue" projects.

In 2007 he had the opportunity to switch to Europol and fight Cybercrime, a form of criminality that is global in nature, from an international perspective.

Jaap has a degree in Technology Assessment and he recently (2011) obtained his Masters in Computer Forensics and Cybercrime Investigations at the UCD in Dublin. The topic of his dissertation is about "cybercriminal organisation".

### **Kenneth Propp**

Kenneth Propp, a senior attorney in the Office of the Legal Adviser, Law Enforcement and Intelligence, U.S. Department of State, has been the Department's lead negotiator for a series of international agreements in recent years relating to law enforcement and border security information-sharing and privacy. These include: 2008 agreements with European Union member states on sharing of biometric criminal history data; the 2007 U.S.-European Union Passenger Name Record (PNR) Agreement; the 2007 U.S.-European Community SWIFT arrangement; the 2007 U.S.-EU Agreement on Security of Classified Information; U.S. agreements with the EU law enforcement organizations Europol and Eurojust; and the 2003 U.S.-EU Mutual Legal Assistance agreement.

### **Guiseppe Vaciago**

Giuseppe Vaciago has been a lawyer and a member of the Milan Bar since 2002 and for the last 10 years his primary focus has been IT Law with a focus on cyber crime. He has assisted many national and international IT companies. Academically, he received his PHD on Digital Forensics from Università di Milano and he is a lecturer at Insubria University (Varese and Como) where he holds a course on IT law. He recently attended Fordham Law School and Stanford Law School as a 'Visiting Scholar' to expand his studies in his own particular research area. He is member of Cybercrime Research Institute based on Koln and Fellow at Nexa Center of Politecnico of Turin. Giuseppe Vaciago is the author of many publications on cybercrime, including both scientific journals and textbooks, which have been adopted by the University where he teaches. He has also delivered many lectures and presentations in both Italy and abroad.

#### **Silvia-Adriana Ticău**

Silvia-Adriana Ticău is a Romanian Member of the European Parliament, from 1st January 2007. She is Vice-Chair of the Committee on Transport and Tourism in the European Parliament, a substitute member of the Committee on Industry, Research and Energy and a member of the Science and Technology Options Assessment (STOA). Prior to becoming an MEP, she was Member of the Romanian Senate (Nov 2004-Dec 2006), Minister of Communications and Information Technology (July-Nov 2004) and Secretary of State for Information Technology (Sept 2001- July 2004). She also served as a General-Director for Information Technology and Information Society Development Strategy at the Ministry of Communications and Information Technology (Jan-July 2001). Before 2001, Mrs. Ticău was Director of Operations, Director of Information Technology Department, Software Director, and analyst-programmer in the private sector.

Silvia-Adriana Ticău is the EP's rapporteur for "A competitive digital single market - eGovernment as a spearhead".

#### **Dr. Marnix Dekker**

Marnix works at ENISA, focussing on cloud security, smartphone security, cyber security in general, and the implementation of the EU-wide security legislation for Telco's (Article 13). He has a degree in Theoretical Physics (quantum mechanics, qcomputing) and a PhD degree in Computer science. His PhD thesis proposes new, more flexible, access control for collaborative work environments such as medical health record systems.

Before joining ENISA, he worked for KPMG in the Netherlands as an IdM architect and an IT auditor. For example, he designed the new version of DigiD, a digital ID for citizens (around 8M users and 40M transactions), and the first version of e-Recognition a delegation system for Dutch businesses based on SAML and XACML. At KPMG he also followed (in a QA role) the deployment of a large cloud and outsourcing service (around 200M euro) for a vital government agency.

#### **Marc Crandall-Google Enterprise**

Marc Crandall serves as senior manager of global compliance, enterprise, at Google, where he addresses security and privacy compliance matters regarding Google's cloud-based services. Marc has also served as product counsel for Google, where he addressed legal issues concerning the development and deployment of Google technology. He has helped ensure compliance with US and international laws and regulations dealing with privacy, law enforcement, system security, intellectual property, content regulation, telecommunications, consumer protection, advertising, and child online protection.

Prior to joining Google in 2006, Marc served as assistant general counsel with the science and technology law unit of the United States Federal Bureau of Investigation (FBI). As principal legal adviser to the cyber division at FBI headquarters in Washington, DC, he provided legal counsel and policy advice concerning issues involving Internet forensics, computer intrusions, crimes against children, counterterrorism and counterintelligence operations, intellectual property enforcement, privacy and white collar crime.



Before joining the FBI, Marc served as corporations counsel and lead counsel of internet compliance and enforcement with the California Department of Corporations, California's investment and finance authority. There, he developed policy and executed legal duties in the field of internet forensics, undercover operations, evidence collection, litigation, and the application of evidentiary, privacy and transactional laws to the internet. He also created and led the State's first team dedicated to combating internet-based investment fraud. During this time, Marc was appointed as a special assistant U.S. attorney with the United States Department of Justice, investigating and prosecuting violations of federal law. Marc earned a Bachelor of Arts degree from the University of California, Los Angeles and a juris doctor from Pepperdine University School of Law. He also holds a certification with the International Association of Privacy Professionals.

**Dr. Carl-Christian Buhr**

"An economist and computer scientist, Dr. Carl-Christian Buhr is a member of the cabinet of Neelie Kroes, the Digital Agenda Commissioner and EU Commission Vice-President. Among other things, he advises her on the forthcoming European Cloud Computing Strategy, ICT standardisation and interoperability, ePrivacy and data protection issues as well as ICT research policy. He previously dealt with Commission antitrust and merger control investigations, for example the Microsoft antitrust investigation and the Oracle/Sun Microsystems merger case."