Openforum Academy

White Paper

The Policy, Legal and Regulatory Implications of Regional Clouds

Report

The Policy, Legal and Regulatory Implications of Regional Clouds

26 November 2014, Silken Berlaymont, Brussels

Speakers

Christopher Millard - Professor at Queen Mary University of London
Hans Graux - Project Editor for the EC Data Protection Code of Conduct for Cloud Computing
Pablo Troyon Rama - Vice President Cloud Europe for IBM

Moderator: Graham Taylor, CEO of OpenForum Europe
Rapporteur: Diana Cocoru, Policy Analyst at OpenForum Europe

Credits:

Disclaimer:

This report was prepared by our rapporteur, Diana Cocoru, for OpenForum Academy (OFA). The summaries of the speakers' introductions and following discussions presented in this report are based on the rapporteur's notes and they are not in any way binding or necessarily complete. 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 or OFA. Neither the rapporteur, nor OFA should be held accountable for any claimed deviation from the original speeches.

OpenForum Academy gratefully acknowledges IBM's sponsoring the costs of the venue and breakfast. OFA welcomes financial support for its events, but always maintains independence of the discussion itself and the follow up White Paper.

Executive Summary

Time and time again people can hear references to "data Schengen area" or "fortress Europe". While some people raise concerns about the negative impact of such regional approach, others consider that reinforcing regional clouds might be the appropriate solution.

During this second event of the OpenForum Academy Round Tables' Programme, stakeholders from industry, European policy-making, academia and community looked at the policy and legal implications of regional cloud. To set up the context, Professor Millard described the historical context and the concept of "balkanisation" of the cloud and then he pointed out the difficulties of defining a "Europe-only cloud". Following his intervention, Mr Graux, the editor of the EU Code of Conduct, described the drafting work and the outcomes of this industry-led non-binding text. Before passing to the interactive discussion with an audience of more than 45 participants, Mr Troyon Rama represented point of view of the industry and conveyed IBM's observations about the shape of the European Cloud market opportunity as well as client feedback on what are their key priorities and concerns, majoring on how of new technologies are powerful enablers of innovation and economic growth.

The audience actively participated in the discussions, addressing several aspects of data storage localisation and its justification. The interventions raised concerns about the consequences of polarised debates, they touched the existing emotional justifications underlying the choices of data centres and also looked at alternative solutions to ensure data protection and privacy. Many of these points found the consensus of the participants to the event.

Table of Contents

Setting up the context

Mr Graham Taylor opened the round table with a short presentation of OpenForum Academy (OFA). This is a think tank created a few years ago, which gathers over 40 fellows among the best innovative thinkers. They are coming from academia and industry around the world and are active on all aspects of openness, providing expert input to OpenForum Europe (OFE). OFE is a not for profit organisation, independent from any single company, promoting openness in the IT market. Although it still remains very active on open standards, it is progressively looking at all the open aspects of IT and particularly at the avoidance of lock-in.

Openness is identified as the mantra of OFE's activities. Being an abstract concept, there are generally few efforts to define what it is meant exactly with "open". This is why OFE has started to develop a set of **high level generic principles of openness**. These principles cover four aspects: user centricity (understanding the needs of the user), competition (ensuring a level playing field), flexibility of solutions (have full interoperability), sustainability and community (an environment allowing people to collaborate). After developing these principles at the theoretical level, OFE then applies them to the practical level. For example, in the context of cloud, OFE is looking to establish a set of principles for an open could, by explaining what this means in real terms. While covering more than technical interoperability, openness is also looking at the commercial and legal aspects of what "Open Cloud" means.

In order to look at the different angles of cloud computing solutions, OFA launched in October 2014 a Program of Round Tables, so as to bring together policy-makers, academia, industry and the community, and debate the implications of the EU cloud strategy and its challenges for the stakeholders. The first such event took place on 10 October, on the topic "Trusted Cloud for the Enterprise – what are the key factors today?". The White Paper is available on OFA's website. The second event in the series is the one reported by this present White Paper.

Mr Taylor pointed out in his introduction that although words like “data Schengen area” and “fortress Europe” are starting to disappear, they still leave the question of what it really means to run a cloud service within Europe. The event brought together three speakers to tackle these issues from different stand points: **Christopher Millard** is Professor of Privacy and Information Law at Queen Mary University of London. Part of his work was funded by the Microsoft Cloud Computing Research Center and it resulted in the paper "Policy, Legal and Regulatory Implications of a Europe-Only Cloud" which content he presented at the event. **Hans Graux** is a lawyer from Time.lex and the editor of the EU Code of Conduct for Cloud Computing. **Pablo Troyon Rama** is Vice-President of IBM's Cloud business unit in Europe.

Panellists' introductory speeches

Each member of the panel made a short introduction, in order to lay down their thoughts on the topic. After setting up the framework, the audience was engaged in an interactive debate.

In his introductory speech, **Christopher Millard** focused on the following points:

- the historical context of the discussion about European cloud;
- the recent trends towards "balkanisation" of the cloud;
- the question of whether cloud localisation makes sense in practice or if other factors are more important;

Regarding the **historical context,** Professor Millard pointed out that discussions about data export controls exist since 1970 and the Swedish national data protection act. He underlined that since then, data localisation has been a hot topic not only in Europe, but also in North America, Canada, Middle East, Asia and China. Over the last 35-40 years, there have been various initiatives to harmonise data protection rules, including both non-binding measures, like the OECD Guidelines, and binding treaties and other instruments, such as the 1981 Council of Europe Convention on Data Protection and the 1995 EU Data Protection Directive. The historic context reflects the ongoing explicit objective to ensure the free flow of data between countries that commit to a certain level of protection for personal data.

As regards **mandatory localisation, or 'balkanisation', of data**, Professor Millard emphasised that, despite the efforts and the good faith of policy makers to ensure free flow of data, **there are still calls for geographic restrictions on data flows.** Although more than a hundred countries now have data protection rules, the focus on geography and jurisdiction has not gone away. For example, there have recently been calls for transfers to be restricted between Europe and other parts of the world, even where there is a legally binding mechanism in place to justify the transfers, such as the US-EU Safe Harbor agreement. Specifically, Professor Millard pointed to calls from the European Parliament, as well as from some EU national governments and regulators, to revise or reform this agreement under which personal data may be transferred from anywhere in the EEA to participating entities in the US. With the Snowden revelations, the issue of whether the Safe Harbor is still 'safe' became a heated debate, leading also to questions as to whether restrictions on transfers within established free flow regions, such as the European Union, might be needed.

When it comes to the origin of a Schengen for data, Professor Millard underlined that this idea did not come from any of the Member States, but from an EU discussion which dates back to 2011, thus taking place before the Snowden revelations. In February 2011, at the meeting of the EU law enforcement and customs cooperation working party "the presidency of the Law Enforcement Working Party presented its intention to promote concrete measures towards creating a single secure European cyberspace with a virtual Schengen border and virtual access points whereby Internet Service Providers (ISP) could block illicit content on the basis of a EU black list.". Continuing this line, in August 2013, Thierry Breton from the EU cloud provider Atos and previously France's Minister of Economy, Finance and Industry, suggested it was time to have a kind of Schengen for data. Later that year, Deutsche Telekom announced its plan to build a German-only internet, to keep German internet traffic within German physical borders. In 2014, Merkel and Hollande met to talk about building up a European communication network to avoid communication and other data passing through the US. On this point, the Professor concluded that this is not a dead issue.

Looking at the practical terms, Professor Millard chose **three US cloud services providers and**

three European cloud services providers, to analyse what they say about data localisation, regionalisation and restrictions on transfers. For the US, Amazon announced that they had launched a "new German region", which joins Ireland to become Amazon's second EU infrastructure location. Microsoft stipulates that "customers may specify geographic areas and regions of the Microsoft data centres in which customers' data will be stored", and Google uses the FAQ section on its Google Apps website to answer to the question "where is my organisation data stored?" by saying that "Your data will be stored in Google's network of data centres", without further explaining where these are or giving a choice to the customer. On the European side, Deutsche Telekom states that it has 90 data centre worldwide and that "the greatest security is offered by the 30 German data centres" and that "customers themselves can decide where their data is to be stored". BT Cloud Compute specifies that they are "letting [the customers] decide exactly where they want their sensitive data to be stored", whereas Jottacloud, a Norwegian cloud storage service, states that it "lets you securely copy, synchronize, save and share files from all of your devices" and that "these files will be safely stored on environmentally friendly servers in Norway or in countries with equivalent or even more rigorous privacy laws. Firms based in the US might be forced to hand over their stored information to the authorities. No one will get access to the data stored with us". This shows the different approaches of cloud service providers when it comes to addressing data localisation concerns.

After demonstrating that the regional cloud approach is not a dead issue, Professor Millard went on to explore how each basic component of the "**Europe-only cloud**" could be defined:

- **'Cloud'** is not one single thing, but an umbrella covering different types of services ranging from Iaas and PaaS, to SaaS. From this angle, the following questions remains open: when one uses 'cloud', is that a reference made to the data centre only, to the entire range of services that run on the cloud stack or rather to the network capabilities? And even when cloud is interpreted widely, is one implying that by encouraging European-only clouds, using non-Europe cloud services should be banned? Would that really mean the blocking of popular services such as Facebook and Twitter with moves to replicated them locally, as has been attempted in countries like China, Saudi Arabia and North Korea?
- **'Europe'.** Europe could be the European Union (28 countries), the EEA (31 countries), the Council of Europe (47 countries) or the Schengen Area (22 countries). Out of the 6 EU countries which are not in Schengen, 2 do not have any intention to join: Ireland, where many of Europe's biggest data centres are located, and the UK, which is a hub for financial services and eCommerce. When trying to define "European" using these geographical-institutional categories, the essential question which remains open is: what needs to be in Europe, in order for the cloud to be considered "European"? For example, is it the headquarters, the activities, or the staff? Or perhaps it is about the physical location of its data centres or the data itself? And what can be said about routing and remote access from outside Europe?
- **'Only'** is the 3rd critical component. Does this qualification imply the obligation to process data only in accordance with EU law? If so, which law or which laws should then be applied? Professor Millard mentioned that the Code of Conduct (CoC) drafted by the Cloud Select Industry Group (C-SIG) states very clearly that if one wants to sign the code, one has to commit to abide by all national laws in the EU that might be relevant for that processing. The challenge is that there are conflicts between national laws regulating the processing of data and the transfer of data even within Europe.

Professor Millard concluded his intervention by addressing the question of whether geography and data location are still important. His observation was that from a technical point of view, physical access to data is neither a necessary, nor a sufficient, requirement for access to information in an

intelligible form. This is because data that are physically located in Europe, but not managed securely, may be accessible from anywhere on the planet. On the other hand, **logical access is both necessary and sufficient to get access to data in an intelligible form, regardless of geolocation.** However, **from both legal and practical perspectives, geography and location can still matter.** If a government or regulator has direct access to legal entities in its jurisdiction, it makes it easier to bring enforcement action against those entities, seize their assets, and even bring individual proceedings against their staff. Professor Millard also addressed, in his concluding remarks, the wrong assumption that if a virtual wall was to be built built around Europe, then the European IT industry would blossom and promote the development of leading European cloud providers to compete globally. He argued that, based on the experience of history, building a virtual wall around Europe, or specific countries or regions within Europe, would be the best way to make sure that domestic industry and innovation wither and die.

Hans Graux took the floor to present the work achieved by the C-SIG Group in the drafting of a Code of Conduct (CoC) for Cloud Computing. He started his intervention saying that the CoC is not a legally binding instrument and that it might not fix all the challenges brought about by the previous speaker.

Before moving on the explain what the Code aims to do, Mr Graux presented **the broader policy context.** The EU has adopted a Cloud Strategy in 2012. It includes several actions that the European Commission wants to undertake, in order to facilitate the use of the cloud computing in order to stimulate the European cloud industry. Mr Graux underlined that the strategy does not include any new regulatory interventions and that its objective is not to legislate new activities or create new barriers. Throughout the code, the only reference to legislation is the one to data protection, which states that work should continue. Under the EU Cloud strategy, several C-SIGs have been created, in order to address the problems faced by cloud vendors and cloud buyers in the EU, including issues like credible service level agreements, which are looking at fair contractual terms and data protection. The C-SIG subgroup on data protection has been working for more than one year on the creation of a code of conduct (the "CoC"). Its approach is to let the industry drive the process, getting them to contribute to solve some of the problems of using cloud computing solutions.

Mr Graux then highlighted a couple of remarks about the initiative. First, **the code is not an initiative of the Commission** and the Commission does not control it and it will not sign on it. The code is an industry-led initiative, created with the help of Industry Groups that have volunteered to participate in drafting it, trying to bundle the best practices in what they think would be reasonable requirements. Second, **it is not a pure soft regulatory instrument**. The objective is to be submitted to Article 29 Working Party, which is the European supervisory body consisting of representatives from all the national data protection authorities. The aim is for the Article 29 Working Party to sign off on the code, with the underlying signification that they agree with the content of the code. When this step is achieved, the message will be that that if the code is respected, it can reasonably be assumed that the cloud service complies with the European data protection law. Mr Graux pointed out that in the past 20 years, there have been multiple attempts to get codes of conduct approved and only once this initiative succeeded. However, those initiatives often failed because it is very difficult to get industry aligned with data protection regulators. Therefore the hope is that the European Code of Conduct will be the second successful initiative which gets approved by data protection regulators.

In terms of **content**, the code presents a set of requirements targeted towards business to business (B2B) contexts. It includes rules on how data subjects can exercise their rights, how the cloud provider is expected to work with the customer and with the data protection authorities and what

happens when these authorities receive law enforcement requests. Other rules that are stipulated in the CoC are the requirements on security. However, those are not phrased in hard terms, because this aspect is impossible to standardize and depends on the type of provisioning model which is provided. For example, IaaS and PaaS are very different than SaaS: some providers might know what type of personal data they process, like for example the healthcare industry would know they are processing personal data and sensitive personal data, thus they are expected to have more stringent security requirements on the data protection front. On the contrary, IaaS providers might not know if there is any personal data on their systems, let alone what kind of personal data. In this context of security requirements, the CoC specifies a series of questions that need to be asked about the nature of the cloud service and it also informs the customer about the kind of security measures that are offered as a service. Mr Graux also emphasised that the CoC does not allow to opt out of the European data protection rules, because it does not grant the right or the possibility to overwrite European rules. It does not create any kind of new particular restrictions either.

Although the code is a voluntary instrument, **there are concerns that this might end up being regulation for the European cloud market or even for the global cloud market**. Mr Graux emphasised that this was not the intention and in any case it could not be legally done. He underlined that the purpose was to have a CoC that cloud providerscan sign up to voluntarily if they see any kind of added value in it. Moreover, the code can prove to be a good market selling point towards the customers.

In terms of **adherence process**, the CoC enables two different schemes for cloud service providers:
1. The code allows CSPs to declare their own adherence, based on the check list made available. In this case, the providers fill in a form to declare that they fulfil the requirements. There is no auditing involved in this scheme
2. The CoC supports a separate certification scheme, where compliance with the Code is checked by third party auditors. The editors of the code tried to make this system as light as possible: every time a cloud provider can present a certification scheme already specified by the code, there will be no further requirements to undergo an additional certification for adherence to the CoC.

In terms of **timeline**, the drafting work started in the second half of 2013 and it can be considered that the current version is relatively mature. The first draft was already submitted to the Article 29 Working Party at the end of February 2014. The C-SIG is now finalising the second version of the CoC, aligning it with some of the requirements of the Working Party. The group plans to submit the second version to the Article 29 Working Party in mid-December 2014.

Mr Graux pointed out that **the goal of the CoC initiative was not to work on an infrastructure that is purely European-only and that creates walls around Europe**. The document is perfectly viable for non-European companies who wish to declare their compliance with the CoC. A confirmation of this point is the fact that in the C-SIG, a lot of the companies are US-based, thus the code would not be limited to European undertakings who can also use data centres which are based all over the world, since there is no restriction imposing that data centres must be located in Europe.

After an introduction from the academic research perspective and a presentation of the policy development of the Code of Conduct at the European level, the audience was introduced with the industry perspective of the implications that regional cloud can have.

Pablo Troyon Rama started by explaining IBM's strategy to help clients extract the benefits of cloud technology, which is based on three pillars. These are: geographical localisation, effective security and continuous innovation. Although the most obvious benefit of adopting cloud solutions

is reducing costs, Mr Troyon pointed out that 90% of clients in Europe today are more worried about top line growth than they are about saving costs, since the opportunities for saving costs are largely exhausted after years of adaptation to the economic crisis.

The first pillar that Mr Troyon addressed was **geographical localisation.** He mentioned that currently IBM has 9 data centres[1] for delivery of public cloud services in Europe, growing to 11 by spring 2015. The reason for this is because clients are demanding the data centres to be available in their home country. This is motivated by organizational culture to a large extent: in certain countries, organisations feel better if they have the data hosted in country and thus can oversee adherence to compliance and regulation on data privacy without obstacles or risk of inconsistent policies due to different regulatory regimes between different countries. The geographical choice has nothing to do with technological capabilities, Mr Troyon considers this will remain so for some time, although culture evolves and new generations may have a different understanding of privacy. In any case, he continued, the geographical choice has to do with the perception clients have about compliance and regulation. He considers there is insufficient clarity about compliance and regulation about the implications of data privacy on cloud and that when clients perceive any risk of legal exposure they opt for the most conservative option available. Thus they try to avoid by all means any legal liability, ignoring that they are held accountable not only when data is hosted in the cloud, but also when data is on premise.

The second pillar of IBM's strategy is **effective security**. Mr Troyon underlined that this was a problem in itself, regardless of whether data is in the cloud or on premise. He pointed out that none of the largest and most notorious incidents of IT security around the world had anything to do with data in the cloud. This is because clients moving sensitive data to the cloud previously go through a very thorough and comprehensive audit on security, covering their software, the processes and the levels of access, which creates the paradox that data hosted in the cloud is typically more secure than the same data hosted on premise under less robust security policies and processes

The last pillar is **continuous innovation**. Mr Troyon emphasised that one of the systemic benefits of cloud technology is that it lowers the barriers of entry for small businesses to start up and participate in the global economy. Nowadays it is very cheap to have access to computing power on a variable cost basis, allowing for a start-up company of 3-4 colleagues, anywhere in Europe to start operating around the world in a matter of days. This environment is highly needed in Europe as new enterprises and job creation will come from newer, technology-enabled industries more than from other more traditional sectors.

Mr Troyon concluded his speech by saying that there should be no compromise between data privacy and economic benefits. Everyone needs a solution that reconciles both. Otherwise, burdening the system with the wrong kind of regulation will only increase the cost. Further he broke down the cost that enterprises need to manage in 4 categories: energy, cost of using and extracting value from data, taxes and talent. He pointed out that if energy on the continent is already expensive, if costs of extracting value from data would be relatively more expensive than in other parts of the planet due to excessive compliance and regulation on data privacy, then it is only with the two remaining variables that businesses can play with, in order to be competitive: cost of talent and taxes. People also have to take into account that when it comes to innovation, there will be 25 million people developing code in 2017 around the world, sky rocketing from around 10 million today. He also added that more and more of those are freelancers. For these people to operate, they need to have, amongst other elements, a technology platform that is affordable, continuously available and flexible. The talent otherwise may move somewhere else.

1 In Paris, Montpellier, Lisbon, London, Barcelona, Wintertur (Switzerland), Germany, Milan and Frankfurt.

Discussion

Disclaimer: These comments were taken from the interactive debate following the introductory presentations and do not necessarily represent any of the speakers' views or those of their organisations. The discussion took place under Chatham House Rule and therefore names and affiliations of participants are not reported.

After addressing the unwanted consequences of polarised policy debates, the participants analysed whether it is security concerns or emotional perceptions which dictate the choice of data localisation. The discussion then concluded with the topic of alternative solutions to looking at geographical data location and the technical benefits of encryption.

The unwanted consequences of polarised policy debates

The first reaction following the three introductory interventions was ringing the alarm about the risks of polarised debates, on a background of already heated discussions and tensed public perception, which culminated with the Snowden revelations.

After offering some clarifications in reply to the statements made by Professor Millard, about the role of expert committees which are not necessarily followed by the Commission, one member of the audience underlined the danger coming from strongly held views about revelations of mass surveillance, badly expressed by Member States and by users of ICT services, about revelations of mass surveillance. This results in a very negative impact on the industry and the users. It was emphasised that one needs to look at the effect of the work of drafting the EU Code of Conduct and at the fact that DG Connect has been sponsoring this industry-led process, which will lead to an industry solution, therefore a solution which the industry can actually apply. This can happen only if the process goes through validation for it to be realistic. This is why the CoC has to be seen and perceived as a valid and legitimate response to the huge levels of concerns expressed publicly, in order to enjoy some weight.

As it was pointed out in the introduction, some IaaS providers have difficulties when signing up to this code, because of the way it is worded. However, it was underlined that those issues are currently being addressed, by making the code provisions more specific and explicit, so that the various activities can be taken into account, without imposing greater obligations.

It was also emphasised that people need to have a more mature discussion about the non-regulatory, the co-regulatory and the self-regulatory approaches. Otherwise the risk is that people just polarise the discussion. The participant to the discussion raised the point that the only winner from such debates was already seen in the first resolution of the European Parliament, after the main revelations of Snowden. When reading that resolution and comparing it with the Commission's communication issued at the end of November last year, it can be seen that the Commission tried to mediate the situation by enabling the consideration of other approaches than strong regulatory impositions, which would have made it more difficult to have data transfers. Moreover, if people are going to take a user centric focus, what is needed is to look at wider users and not just business users.

Another participant intervened to point out that the polarisation is not only between different categories of stakeholders, but exists inside the Commission itself. It was underlined that the approach taken by DG Connect over the last two years had been largely in favour of free data flows. The participant exemplified this argument by quoting Ms Neelie Kroes, who said "I have a dream of a transatlantic market for technology services". This was in response to Viviane Reding (then DG Justice Commissioner), who had said the following, in the context of TTIP negotiations: "I warn against bringing data protection to these negotiations. Data protection is a fundamental human right, it is not negotiable. The Americans need to change their law to get in line with Europe."

To support the point made about the danger to polarise the debate, another participant to the discussion made a point about the territoriality law enforcement access. It was underlined that the Snowden issue was not only a US debate, but also a EU debate. The participant encouraged everyone to engage in a more profound and in depth debate on the tools that are currently available in order to overcome those issues, like how one can access personal data, the territoriality, the sovereignty needs of nations states and the benefits of the cloud. It was emphasised that in these topics the EU can and should help, when it comes to the internet jurisdictional paradigm shift. The participant also mentioned the European investigation order, which is one piece of the puzzle. Besides this, since 2010 there are ongoing negotiations with the US, on an agreement for law enforcement purposes and data protection. These are topics which need further debates. To add to this, if one thinks about the forthcoming digital single market and the overall revision of the telecommunication framework which will include a debate on widening the scope, then one will have to address not only data access issues, but the whole Pandora box of data retention obligations for law enforcement purposes and interception. All those elements will be problematic in answering those questions of perceptions and the view that the law enforcement community has, in not being able to fulfil the users' safety requirements.

While mentioning that the polarisation happens within governments' own communities just as much as within the Commission, the conclusion was that only if people can find ways to stop the polarisation within our continent, will they be in a better position to do it across the Atlantic.

The real motivation behind the choice of geographical location of data storage

Before looking at the motivations which dictates the choice of the data location, participants to the discussion mentioned some visible trends in adopting cloud solutions.

A representative from the industry took the floor to give more insight about their initial approach to data localisation, when work was done on the CoC. According to the participant's intervention, when they started offering these services, they were surprised to see that the benefits that companies were interested in about when adopting cloud services were first in scaling down rather than up. Companies were not willing to invest in IT infrastructure or software, because they wanted to build a business quickly with minimal initial investment. To continue talking from experience, the participant explained that it was complicated at the beginning, because people liked to have their IT infrastructure in their company. Not even in the same country, but on premise. At that time, remote servers that were not on the premises were not acceptable.

From the perspective of this business representative, it also appeared that the adoption of cloud happened in small companies in Spain, Italy and those countries that were lacking the money to invest in IT cloud infrastructure because of the economic recession. This seemed counter intuitive, as one would have expected cloud services to be a tool for flexibility and competitiveness for big

companies and not necessarily a motivator for small companies.

Moving to the more substantial debate of data location, someone raised the point that Russian companies are asking for their data centres to be hosted outside the EU, namely in Switzerland, because they do not trust the EU and they do not trust America. However, the speaker went on, when looking at the level of security of protection that one can have in a traditional setup (on premise data centres owned by the client), there are examples even of large companies, who when being asked where the documentation of enterprise architecture or their infrastructure model is, very few actually have those documents. And these examples include some of the top 20 banks in Europe. The problem is that no one is looking into that, although **it is an established fact that the weakest link is the network.** That is where one hacks to take data, not in the physical machine where the data is stored. To illustrate this, the participant mentioned that nowadays the largest banks in Paris move 80% of client data or client base daily, routinely, between Geneva and London through public networks. The person pointed out that it is strange that for some reason, the alarmist perception exists in relation to cloud solutions, when **the real issue is actually data security, regardless whether it is in the cloud or not.**

Another participant re-emphasised that it is security that people should be focusing on. This is because one can have the data in Europe, but it can totally be insecure and accessed from outside Europe or one can have the data anywhere on the planet and totally secure. Therefore the question is not primarily geographical location. However, there tends to be a consensus that this is an emotional discussion and this is why there is so much politics in it. Particularly in the public sector, a lot of the governments state that they could move to the cloud, but they would have to be assured that the cloud will be in their country. Not in the EU, but in their country. This exemplifies the emotional aspect of the choice, which tends to play a bigger part than economic considerations. This is because politicians do not want to have to stand out and apologise in case there is a data breach.

Another participant took the floor to state that there are other aspects to the security than where the data is stored. All things being equal, the person stated that there are fewer risks posed to the data stored in the EU because it has safeguards not available to countries outside of the EU. In reply to this point, it was said that **location is not the most important aspect, security is, and the worry should be how secure one's data is, not its location**. To counteract this, another participant expressed that **location is part of security**, thus one cannot say location on the one hand and security on the other.

Throughout the debate, there was a general agreement that people do not want their data to be exploited without their consent. It is a well known fact that data has economic value, regardless of it being hosted at the data centre of the bank, under three layers of security or hosted somewhere in Iceland. The main concern for the end users is for their data **to be secure anywhere.**

In reply to what was said about reducing the risk and security, a representative from the business made the remark that people are mixing up the issues. To explain this standpoint, it was said that the General Data Protection Regulation (GDPR) is reducing the risk of how companies misuse data, but the same discussion is happening on government surveillance and hacking the data. So **the real question is what do people want to achieve?** If they want to reduce risk of how companies use data, then they have to rely on the GDPR. If people want to reduce the risk of how governments access data, then this should not be mixed up with the commercial value of data in the same part of the negotiation. That should be a government to government discussion on surveillance and things should not be dragged together in a topic such as the Safe Harbour, because that is not the right forum to have such a discussion. Government surveillance is linked to security and encryption. In

this context, localisation of data does not have any influence. Hackers and governments, both can have access to data, it is all about the encryption that companies could use to keep data safe.

The availability of alternative solutions and the way forward

The discussions turned to the fact that in this entire debate about internet, there appears to be a conflict between the value of privacy and freedom and their monetisation. It was said that despite the fact that the internet seems free, when we look at Facebook, YouTube and the like, the real price that people pay is with their privacy and data (through accepting some conditions of services that users never take the time to read before they agree). Therefore the question which set the scene for the discussion was the following: **how can we make privacy and growth go well together, without compromising any of those?**

There was agreement that there are some competing interests, but these do not limit only to privacy and monetisation. One should also add the freedom of expression. It was stated that this was not something that people had yet learnt how to manage very well in Europe. Whereas in the US there is a very strong tradition of freedom of expression, some would say it is too strong and not balanced well with privacy, while in Europe it tends to be the opposite. The speaker pointed out that in the so-called "Right to be forgotten" case, the ECJ did not make any serious attempt to balance freedom of expression and privacy. Thus the question raised was: who should be making this difficult decisions about privacy and freedom of expression?

This led to other remarks, stating that the current privacy rules are anyway not being complied with. Taking a very practical example, someone brought the argument that anyone who is flying from Europe to New York, with the current state of the art technology device, could export thousands of emails, contacts and personal data. Will that traveller be expected in the future to get permission for this data transfer? Will that person be expected to get an export license? Although this remains trivial compared to the massive industrial scale movements of personal data in the public sector and the private sector every minute of every day, this actually goes back a long way with the philosophy of law and jurisprudence. That is to say that a law people cannot comply with even when they try to, **is a bad law**. The speaker stated that most data transfers are illegal at the moment. Considering that many companies have been spending millions of Euros trying to comply with the laws in the past 20 years and that this proved impossible, the questions which was raised was why perpetuate this with the currently proposed data protection regulation?

This question opened the debate around what counter proposals could be made, that might prove to be better than what it is available now at EU level. The person who took the floor underlined that one of the major needs is to better align internationally at how these topics are addressed. In the current set up, it was said that data export rules are actually a way of trying to export European values based on the reasoning that Europeans think that these safeguards are important, therefore before allowing to exploit data, one should acknowledge that it is important to first deal with those various restrictions.

Trying to come with an example of how things could be done differently, someone suggested to look at the example of Canada. In 1972, a Canadian Federal Government report acknowledged that "as a sovereign state, Canada feels some national embarrassment and resentment over increasing quantities of data about Canadians being stored in a foreign country [the US]". Given such concerns, Canada could have adopted a very locked down approach to data exports, but it chose instead another route. The current Canadian Federal Law does not rely on geographical restrictions

on transferring data. They use **accountability** instead. Thus for them it is not important where data is located but rather **who is responsible**. In this framework, transferring data inside Canada is no different than transferring data to China, when it comes to accountability. The speaker acknowledged that there are accountability provisions in the proposed European regulation which could be helpful, while noticing that they were not replacing bureaucratic export controls, but they were adding to them. The bottom line of this intervention was that **accountability should matter more than geography.**

This argument seemed not to reach consensus in the audience. The person who subsequently took the floor expressed the view that these did not seem to be diametrically opposite approaches. Europeans can also transfer data anywhere, but there are some requirements that need to be met. The issue is the same even for Canada, who also has export controls requirements, except that they are written in terms of accountability in general, whereas the EU is more procedural. To continue the argument, the speaker underlined the added-value of the European standard clauses: there are a lot of customers using them, along with international cloud providers who are using them as standard solutions. The speaker pointed to the fact that even when European standard clauses are the ones being used, the Canadians are satisfied as well. This speaker concluded by saying that the fact that the European model is used, is also a way of showing accountability. The key idea was that in Europe people approach accountability in a different way and argument it procedurally.

Another intervention emphasised that **there should be more clarity on the topic of accountability, because there is too much confusion surrounding it**. People do not understand what they could be personally held accountable for. Besides the companies or organisations, some are even concerned they might be personally liable because of data breaches or issues with sensitive data that is being hacked and that they are supposed to oversee. This point was not necessarily an encouragement to make things harder or more difficult for people, but to emphasise the need to make it clear who is accountable for what.

Although much of the discussion focused on the policy and legal implications of regional clouds, a participant to the discussion pointed out that **we cannot solve everything with law.** Some concerns could also find their **answers in technical solutions**, which sometimes could be even better suited than the legal/political approach.

In the broader policy issue, it was stated that data protection and privacy are not EU-only or US-only situations. The participant to the discussion pointed out to some major security breaches which took place in Belgium over the last year and a half and which were conducted by GCHQ, from the UK. It was underlined that this was not a secret and that it was reported in the press. This example was given to show that everyone has an obligation to work on these issues. It is a policy issue, not a data protection issue. The speaker deplored that all countries have a strong tendency to rely on national security justifications and disobey the rules where a national security situation arises. In such cases, they appear to consider that national security is more important than the fundamental rights. In this setup, the participant went on to mention the two tracks that need to be followed. First, there are the voluntary initiatives like the CoC, which make cloud computing easier, more transparent, more usable, with more due diligence and accountability. Second, there is the public policy issues which require some serious renegotiations that need to take place at international level, including on issues like national security. As long as countries both inside the EU and outside consider that national security is a national competence and that it motivates the willingness to enact rules on the cloud, the major current concerns will not disappear. Besides policy solutions, these concerns can also be addressed through technical means. The speaker stated that encryption offers the ability to protect against surveillance, against hostile attackers even if

those include governments, while the policy initiatives help to make sure that society works the way it should work.

Concluding remarks

This event looked at the rationale behind choosing specific geographical locations for data storage, while also questioning whether location is the appropriate aspect to take into account, instead of security, accountability and encryption.

The EU Code of Conduct that has been drafted starting in 2012 and which reached a very mature version seems to answer to some of the concerns raised during the discussions. Being an industry-led initiative, hopefully soon to be endorsed by Article 29 Working Party, it might have what it takes in order to address users' and governments' requirements addressed to cloud service providers.

The numerous interventions from the audience could be summarised in three main ideas. First, there is a high risk of negative impact coming out of polarised debates, second, the geographical location of data storage is still partly dictated by emotional reasons and third, accountability and encryption might be better solutions than restricting the physical location of data, in order to ensure security. The discussion also emphasised that citizens, businesses and governments alike have an equal responsibility to raise awareness of these issues and to contribute to the wider efforts aimed to ensure data privacy and protection, in order to enable the full benefit of the advantages of cloud computing solutions.

Speakers' Biographies

Christopher Millard is Professor of Privacy and Information Law at the Centre for Commercial law Studies, Queen Mary University of London, has led the QMUL Cloud Legal Project since it was established in 2009. He is a founding editor of the International Journal of Law and IT and of International Data Privacy Law. He is editor and co-author of Cloud Computing Law (Oxford University Press, 2013).

Hans Graux is an ICT lawyer at the Brussels based law firm time.lex, a firm that specialises in telecommunications, IT/IP, media and e-business. He is the Development Leader – Project Editor for the EC Data Protection Code of Conduct for Cloud Computing. In addition, he is an independent advisor to the Flemish Supervisory Council, which supervises data protection compliance in the public sector.

Pablo Troyon Rama currently is Vice President Cloud Europe for IBM and ha held a variety of roles within Spain, Europe, and Growth Markets across IBM. Being a member of the Executive Leadership Team of IBM in Europe, he brings more than 15 years of global leadership and IT infrastructure knowledge to his current position.