Who controls the cloud?

Leenes, R.E.

Published in:
IDP: Internet, law and politics e-journal

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monograph «6th IDP Conference. Cloud Computing: Law and Politics in The Cloud »

ARTICLE

Who Controls the Cloud?

Ronald Leenes

Submitted: July 2010
Accepted: September 2010
Published: December 2010

Abstract
This article addresses some of the data protection issues at stake in cloud computing: more specifically the question of responsibility regarding personal data processing in cloud computing scenarios from an EU perspective. How are the different schemes to be assessed in light of Directive EU/95/46? And are the notions of data controller, data processor, and data subject, as defined in this Directive, still useful? The conclusion of this analysis is that cloud computing scenarios have to be assessed on an individual basis and that the protection the Directive offers to data subjects is often unsatisfactory.

Keywords
cloud computing, privacy, data protection

Topic
Cloud computing

¿Quién controla la nube?

Resumen
Este artículo trata sobre algunos de los temas de protección de datos que se cuestionan en computación en nube. Concretamente, aborda la cuestión de la responsabilidad en el tratamiento de datos personales en situaciones de computación en nube. Aborda esta cuestión desde la perspectiva de la Unión Europea. ¿Cómo deben evaluarse modelos de computación en nube diferentes por lo que respecta a la Directiva 95/46/CE? y ¿siguen siendo útiles los conceptos de responsable del tratamiento de datos, encargado del tratamiento de datos e interesado o titular de los datos tal como se definen en esta Directiva? La conclusión de este análisis es que las situaciones de computación en nube se tienen que evaluar de forma individual y que la protección que se ofrece a los titulares de los datos o interesados en la Directiva suele ser insatisfactoria.

Palabras clave
computación en nube, privacidad, protección de datos

Tema
Computación en nube

Introduction

Every so often the computing industry is shaken by a new paradigm. In the nineteen sixties and seventies, dumb terminals were connected to mainframes, and in the eighties the PC shifted work from the mainframe to the desktop. In the nineties, we witnessed the large scale adoption of the Internet, which not only allowed people to shift from their limited environment of the desktop and venture out in the World Wide Web, but also made it possible to reconnect to the enterprise mainframes and IT infrastructure. Early in the new millennium, grid computing seemed to be the next thing, but currently this is being overshadowed by 'cloud computing' (CC). This is seen by some as revolutionary: "We're moving to a new world. It's about next generation applications and next generation platforms",[1] while others are much more reserved: "Clouds are water vapour. [...] All it is, is a computer attached to a network."[2] Analyst firm Gartner seems to agree with the latter and identified cloud computing as being at the "peak of inflated expectations" and on its way to the 'Trough of Disillusionment'.[3]

Irrespective of whether CC is radically changing the computing landscape, it is a fact in the lives of many employers, employees, customers and citizens. Services and indeed entire computing platforms are transferred to 'the cloud', meaning that data processing and storage locations become fuzzy: rather than data being stored in the enterprise's own databases or in the user's own PC, data in cloud environments can be anywhere on the globe. And worse, the data may move in an instant from one country to another for efficiency reasons: data are indeed in the cloud. This raises numerous legal questions regarding data protection, confidentiality, intellectual property, etc.[4] The nature of CC also questions the foundations of data protection, based on the idea that personal data is processed by data controllers whose location was assumed to be known (Leenes, 2008b, p. 360). The Data Protection Directive 95/46/EC[5] (DPD) aimed to set the rules for processing personal data with (large) IT systems of enterprises and governments in mind. The cloud model may be at odds with this.

This article addresses some of the data protection issues at stake in cloud computing. More specifically it addresses the question of the responsibility regarding the processing of personal data in CC scenarios. I will address this question from an EU perspective. How are different CC schemes to be assessed in light of the DPD? And are the notions of data controller, data processor, and data subject as defined in this Directive still useful?

First, there is a very brief overview of the core concepts in the domain of CC. Next, I briefly outline the DPD, focusing on the concepts of personal data, data subject, data controller, and data processor. Then we will assess different CC scenarios in view of these concepts. The analysis shows that these scenarios have to be assessed on an individual basis and that the protection offered to data subjects by the Directive is often unsatisfactory. Consequently, users of cloud services may want to resort to contracts and service level agreements in order to mitigate some of the risks. Finally some conclusions and recommendations will be given.

Cloud computing

Cloud computing is hard to pin down. It encompasses a multitude of different service and deployment models. An established definition seems to be lacking, although the NIST definition seems on its way to become the de facto definition: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Meil and Grance, 2009). For our purposes, only a few aspects need high-

1. Salesforce's Marc Benioff, see: http://www.zdnet.com/blog/btl/salesforces-benioff-clouds-arent-in-a-box/39488
2. Oracle's Larry Ellison, at the same conference where Benioff lauded Cloud Computing. For his entire speech, see: http://venturebeat.com/2009/10/01/larry-ellisons-annual-cloud-computing-smackdown/
3. See: http://www.readwriteweb.com/archives/gartner_hype_cycle_2010_cloud_computing_at_the_pea.php
4. For an overview of legal issues see, for instance Catteddu and Hogben, 2009 and Van Gyseghem et al., 2010
5. Directive 95/46/EC of the European Parliament and of the Council, 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23 November 1995.

lighting. The most important is the fact that the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model.

The different physical and virtual resources are dynamically assigned and reassigned according to consumer demand. The customer generally has no control over or knowledge of the exact location of the resources provided, but may be able to specify location at a higher level (e.g., country, state, or data centre) (Meil and Grance, 2009).

Cloud services concern resources such as storage, processing, memory, network bandwidth, and virtual machines. Generally three types of services are distinguished: cloud software (SaaS), cloud platform (PaaS), and cloud infrastructure (IaaS). In the case of SaaS, the consumer uses an application provided by the cloud provider. Well known examples are Google Docs, Microsoft's Hotmail and Dropbox. In the case of PaaS, the cloud service provider has a platform for application or service development on which customers can build their own application or service. An example is Vtravelled, a travel service developed by Virgin Atlantic running on the Amazon AWS platform.[6] Finally, IaaS allows customers to run any software, including operating systems and applications on the service provider's equipment. Regarding deployment models, a distinction is made in infrastructures operated for a single organisation (private cloud), cloud infrastructures shared by several organizations and supporting a specific community that has shared concerns (community cloud), public infrastructures and hybrid clouds. Obviously, customers have more control in private clouds than in public clouds which, by their nature, have to have general terms and conditions.

Here, some simple examples guide the analysis. The cases differ as to whether they concern public or private clouds, the location of processing and data storage, and the extent to which the end-user has control over the service offered. I limit the analysis to SaaS cases, because these already illustrate the intricacies of regulation of the different actors and services offered. The first example concerns Eleni Primero, a student at Tilburg University, which has recently decided to use the Microsoft Live@Edu[7] environment for their students. In this case, the service is provided by servers hosted within the EU (Amsterdam, with a backup in Ireland).[8] This is an example of a private SaaS.

The second case concerns the author using Google Docs and other Google Apps to collaborate with partners in a European project. This is an example of a public SaaS. Google cannot specify the location of the servers for this particular case.

The third case concerns Tim Third, who has a Facebook profile hosted by a public SaaS, most likely located in the USA.

Within each CC scheme we can distinguish different entities:

- The service provider (CCS), which is the natural or legal person providing the service (SaaS, IaaS, or PaaS) in a CC system.
- The subscriber/customer. The natural or legal person contracting the CCS. The subscriber can be an individual, such as Tim Third, or an organisation, such as Tilburg University.
- The (end-)user. The natural person who actually uses the CCS in a specific context. The user may coincide with the subscriber, as in Tim Third's case, but may also be someone else. Eleni Primero is the end-user of the mail service contracted from Microsoft by Tilburg University.

These entities can be mapped to concepts in the DPD.

The Data Protection Directive 95/46/EC

The DPD, enacted in 1995, aims to facilitate the free flow of information while maintaining an acceptable level of

6. See http://www.vtravelled.com
7. http://www.microsoft.com/liveatedu/free-email-accounts.aspx?locale=en-US&country=US
8. This was an important factor for Tilburg University to opt for Microsoft rather than a competing offer by Google, which could not guarantee the location of the servers. For similar concerns, see Yale's hesitation to switch to Google mail, http://www.yaledailynews.com/news/university-news/2010/03/30/its-delays-switch-gmail-community-input/

privacy for individuals.[9] It tries to strike a balance between competing interests. On the one hand there is a clear privacy interest of the individual, while on the other, there are freedom of expression and commercial interests in providing services for which personal data are essential. The obligations for the parties involved in the processing of personal data have to be seen in view of these two, potentially conflicting, aims of the directive.

The DPD lays out a number of basic privacy principles that need to be guaranteed when personal data is collected or processed by what are called 'data controllers'. A central concept in the Directive is personal data, which, according to article 2 (a) means any information relating to an identified or identifiable person (data subject). 'Identifiable' is every person "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, mental, economic, cultural or social identity". In consumer-business relations, directly identifying data, such as name, and indirectly identifying data, such as telephone or other numbers, (e.g., customer numbers and social security numbers) are relevant.

We have to assess whether the data involved in CCS scenarios is personal data in view of the DPD. This is the easy question. In many cases, personal data will be processed. All three scenarios outlined in the previous section involve large amounts of personal data.[10] Email addresses (of both sender and recipient) and any content that refers to identifiable people are personal data, but so is, generally, the IP addresses of the equipment used in the various settings and the cookies set by the providers.[11]

Data subjects in CC schemes can either be the user whose personal data (such as account information, IP addresses, cookies, e-mail addresses, preferences, use patterns, attributes) are processed, but also others who are mentioned, or referred to, in particular content such as comments or tags on social network sites, or images portraying identifiable individuals.[12]

Article 2 (b) of the DPD states that processing of personal data "shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Once again, it is not difficult to see that many CCS process personal data.

Data Controller

More difficult are the concepts of 'data controller' and 'data processor'. According to article 2 (d) of the Directive, controller applies to "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law". In article e, the processor is defined as the entity that "processes personal data on behalf of the controller".

Which entity has to be qualified as data controller is relevant for two reasons. First, it determines whether or not the Directive is applicable in a particular case (applicable law), and second it determines who has certain responsibilities and obligations (allocation of responsibility).

The applicability of the DPD is determined in article 4 of the Directive, which states:

> "(1) Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

9. DPD 9 preamble article 3.
10. See also Catteddu and Hogben, 2009.
11. See, for instance, Article 29 Data Protection Working Party, 2007; Leenes, 2008a
12. See, for instance, Kuczerawy, 2010; Article 29 Data Protection Working Party, 2009

> b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
>
> c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
>
> (2) In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself."

This provision distinguishes between controllers physically (1a) or legally (1b) located in an EU member state, or, if located outside the EU, those making use of equipment for purposes of processing personal data except when solely transmitting data from Community territory to a third country, which excludes routers etc. (1c).

In the days before the Internet, this provided sufficient guidance. Usually, the equipment used for processing personal data (mainframe, minicomputer, or PC) was at the location of the entity responsible for the processing (e.g., a hospital or a company headquarters) in which case the controller could be easily determined. But this is less simple today, as illustrated in the cloud scenarios. Tilburg University uses Microsoft services. Microsoft has its main headquarters in Redmond USA, but also has offices in many other countries. Their cloud computing facilities are also in different countries, possibly at the same locations as their offices, but more likely in other data centres. In more complex cloud scenarios, third parties are involved in the service environment. For instance, in the Facebook case, there are advertisement aggregators involved, as well as providers of applications that run within the Facebook environment.

In other words, the location where decisions are taken concerning "the purposes and means of the processing of personal data" does not have to coincide with the location where the actual processing takes place, and there may be multiple entities involved in taking decisions regarding different purposes, meaning that there may be multiple controllers (and processors) in the different cloud computing scenarios.

What determines who the controller is: the location of the legal entity responsible for deciding on 'purposes and means' of the processing of personal data, or the location of the actual processing? If the legal entity is decisive, then in the Eleni Primero case, it does not matter where the data of the Tilburg students is stored, as long as their contracting party is located in the EU (which is the case: Microsoft Netherlands), the students' data is protected under the EU DPD. However, if the location of the processing is decisive, then it may matter where the data is processed and stored.[13]

The Enisa report on cloud computing benefits and risk (Catteddu and Hogben, 2009, p.100) concludes, on the basis of article 4 of the DPD, that the place where the controller is established is relevant to the applicability of the DPD,[14] and that the place of processing of personal data and the residence of the data subject are irrelevant in this respect.

This corresponds to the Article 29 Data Protection Working Party (WP) opinion on applicable law (WP 56) (Article 29 Data Protection Working Party, 2002, p. 6), which states that the "directive uses the criterion or 'connection factor' of the 'place of establishment of the controller' or, in other words, the country of origin principle typically applied in the Internal Market."

Furthermore, "the place, at which a controller is established, implies the effective and real exercise of activity through stable arrangements and has to be determined in conformity with the case law of the Court of Justice of the European Communities. According to the Court, the concept of establishment involves the actual pursuit of an activity through a fixed establishment for an indefinite period.[15] This requirement is also fulfilled where a com-

13. I do not include the applicability of foreign (non EU) law. For instance, if the data is stored on US territory, the USA Patriot Act applies, which has far-reaching consequences. Content that is permissible under EU law may not be permissible in the US, meaning that EU citizens might run a risk when their data is stored in the US.
14. See also Article 29 Data Protection Working Party, 2002, p. 6, which states that the "directive uses the criterion or 'connection factor' of the 'place of establishment of the controller' or, in other words, the country of origin principle typically applied in the Internal Market."
15. Case C-221/89 Factortame [1991] ECR I-3905 §20

pany is constituted for a given period." To make clear that the Working Party do not mix up legal entity with location of the technology it adds: "The place of establishment of a company providing services via an Internet web site is not the place, at which the technology supporting its web site is located or the place at which its web site is accessible, but the place where it pursues its activity".[16]

Opinion WP 169 (Article 29 Data Protection Working Party, 2010) adds "being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes" (p. 8). In this Opinion, a distinction is made between control stemming from explicit legal competence (e.g., appointment by national law), implicit competence (e.g., employer in relation to data on employees), and control stemming from factual influence (facts of the case). The latter category seems most relevant in cases of CCS.

Using the place of establishment of the controller as the decisive criterion, instead of place of processing, does make sense. The decision on what to process and for what purpose affects data subjects the most. That the actual processing of these data, in order to provide a particular service at a certain moment in time, might be done more efficiently or effectively at location X, whereas moving all data to location Y does not really matter for the data subject. Or does it? As the data controller has a responsibility to provide adequate security measures, the actual location of processing and storage does affect the data subject, but arguably to a lesser extent under normal conditions.

However, this is not the end of the story.

In the case where the controller is situated outside EU territory, the 'country of origin' connection factor does not determine which legislation is applicable. In this case, as stated in Article 4, 1 (c) of the Directive, the location of the processing equipment is what counts. In other words, if the controller residing outside the EU makes use of equipment for the processing of personal data situated within a Member State, then the DPD still applies and it is the Member State's legislation that governs the data processing.

Establishing that a CCS processes personal data and decides on the purposes and means of the processing of personal data is, even in cases of entities not residing in EU territory, often not that difficult. Facebook, with its headquarters in Palo Alto, California, determines what data to collect from its users. Google, also in California, determines what personal data to process in the case of Google Apps, and Gmail. But do these CCS providers make use of equipment in an EU member state if an individual on EU territory uses their services? What is the requirement to make the DPD applicable to their operations in the EU? It depends. As stated in Article 4, 1 (c), the equipment has to be used for the processing of personal data, mere transmission tools are excluded.

If the user solely uses a browser to enter data into forms on web pages provided by these controllers, the answer is no, they are not using equipment in an EU member state. The user's PC is then only used for transmission, just like routers, switches and cables. But this changes when these CCS providers make use of cookies, JavaScript, Flash code, etc. For instance, in WP 56 (2002, p. 10-11), the Article 29 Working Party argue that "the user's PC is equipment in the sense of Art. 4 paragraph 1 lit. c Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data, [...]. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory. The Working Party is therefore of the opinion that the national law of the Member State where this user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk."[17]

The last sentence sounds like an oxymoron – *collecting* data *by writing* data on the user's PC, but the cookie is in fact used by the service provider to recognize the user and be able to link his behaviour over time. But still, equating

16. Directive 2000/31/EC, Recital 19
17. This opinion has been confirmed in the Art. 29 WP Opinion on search engines (Article 29 Data Protection Working Party, 2008) and the Art. 29 WP Opinion on Social Network Sites (Article 29 Data Protection Working Party, 2009).

cookies with equipment seems far fetched. This may be a language issue;[18] earlier versions of the Directive used the term 'means', which is closer to what cookies are than equipment which relates to tools and devices.

Cookies raise a more important issue, however. As already mentioned, if the CCS did not use cookies in their services (nor JavaScript, etc) then they would be exempt from the DPD, whereas if cookies are used, the CCS fall under the scope of the DPD. Aleksandra Kuczerawy (2010, p. 80-82) provides an interesting analysis of this with regard to social network sites. Article 5 (3) of the Directive on privacy and electronic communications 2002/58/EC states that service providers may only store information or gain access to information stored in the terminal equipment of a subscriber or user on condition that the subscriber or user concerned is provided with clear and comprehensive information, in accordance with the DPD, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller.

This provision is meant to protect European citizens. Paradoxically, if a user in the EU chooses to block cookies, the protection provided on the basis of Article 4, 1 (c) of the DPD is no longer applicable.

If a CCS provider located outside EU territory serving customers within the EU has to be qualified as data controller (for instance, because it uses cookies), then it has to comply with the data protection regulation of each of the member states served.[19]

Household exception

The DPD contains another condition for applicability of the Directive: the household exception articulated in Article 3 paragraph 2: "This Directive shall not apply to the processing of personal data by a natural person in the course of a purely personal or household activity." This condition is relevant in the light of cloud services used by individuals, and particularly in the case of individuals using social networking sites.

In the Lindqvist-case[20] in 2003, the European Court of Justice decided that: "The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data" and that "Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46."

The Article 29 Working Party, in line with the Lindqvist case, hold the opinion that when users make data available to a high number of third party, possibly unknown, contacts, it may mean that the household exemption does not apply, and the user could be considered a data controller. If the user acts on behalf of a company or association, the household exception does not hold.

Consequences

Defining the exact roles of the parties involved is important because it determines the responsibilities of these parties regarding the processing of personal data. Applicability of the EU data protection regulation means, among other things:

- The controller has to clearly define the purpose of the processing as one of the requirements to make the collection of personal data fair and lawful (Art. 6 DPD);
- The controller has to ensure that the data are adequate, relevant and not excessive in relation to the purpose for which they are collected (Art. 6 DPD);
- The collection must be based on legitimate grounds (unambiguous consent, performance of a contract, compliance with a legal obligation, in pursuance of legitimate interests of the controller etc.) (Art. 7 DPD);
- The data subject has the right of access to and the rectification or erasure of their personal data (Art. 12 DPD);
- The data subject has at least to be informed about the identity of the controller and representative if any, the

18. See footnote 22 in WP 56.
19. Which has been termed an 'impossible burden' (Kuner, 2007).
20. C 101/01 (2003)

purpose of the collection, the recipients and about their rights (Art. 10 DPD);
- The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. (Art. 17 DPD).

Who controls the cloud?

Let us now return to the CC scenarios outlined earlier to qualify the different actors in relation to the concepts discussed in the previous section.

It turns out that in many CCS scenarios there is a plurality of controllers and processors that have either joint or sequential control. The same entity may be controller for one purpose of data processing and a processor for other purposes. The subscriber may be data controller, data processor, or data subject. The end-user may be a mere data subject, but in some cases the end-user may also be qualified as data controller.

In Eleni Primero's case, for instance, Microsoft is a data controller (as they process her account data, and also if they use her data for other purposes), but Tilburg University can also be qualified as data controller because they place Eleni in Microsoft's 'hands'. In the processing for which Tilburg University can be considered the data controller, Microsoft acts as processor.

In Tim Third's case, Facebook is a data controller, but if Tim makes information about identifiable individuals available to a sufficiently large audience, he is controller for this information too. If the information is only visible to his small group of friends, the household exception applies to his actions. The author of this article may be a data controller if he processes personal data, provided that he chooses purposes and means. The household exception does not apply here, because he operates on behalf of his employer. If his employer, Tilburg University, determines that he has to use Google Apps for specific purposes involving personal data, for instance grading papers uploaded to Google Apps, then Tilburg University may be the data controller and Google merely the processor.

What these examples show is that a very diffuse landscape may arise in CCS scenarios, despite the fact that the Directive aims to ensure that, "even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a 'negative conflict of competence' and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties." (Article 29 Data Protection Working Party, 2010, p. 22).

I am not so sure that responsibilities can be clearly allocated. In many (public) CCS scenarios where users have accounts, cookies and inline scripts are used, the service incorporates third party functionality (e.g. applications provided on Facebook) and services (e.g. adverts served by a third party) and the user discloses information about third parties, the complexity may be significant and entities will (try to) shift their responsibilities to others.

But even if responsibility can be clearly allocated, what is the practical significance? Does it lead to an adequate level of protection of EU citizens? What does it mean if the end-user is qualified as a data controller? How, for instance, is the end-user to comply with the security measures imposed by Article 17 of the DPD in such a case? Or how can he comply with the purpose limitation requirement imposed by Article 6?

How much control does an end-user have in situations where 'take it or leave it' regimes exist, as is commonly the case in public cloud services. End-users have a very weak bargaining position against large CCS providers such as Google, Facebook, and Microsoft.[21]

Subscribers, certainly in the case of legal persons, can try to negotiate terms that allow them to comply with

21. And even the Article 29 Working Party seems to have only limited influence on organisations such as Google and Facebook judging from the lax adoption of WP 29 recommendations.

their own obligations, but even here there is a power imbalance between the (usually large) cloud providers and weaker customers (see for instance Catteddu and Hogben, 2009, p. 97-98).

The predominant question is whether cloud computing, with its plurality of involved entities and the fluidity of data and processing, marks a clear need to reconsider the core concepts and roles in the Data Protection Directive? Does the 'territoriality' of data protection rules have to be defined differently depending on the duties (e.g. security or transparency) and the actors (data controller or data processor) at stake, and if so, how (Poullet et al., 2010, in press)?

Conclusion

In this paper, I have provided a glimpse of the basic data protection issues surrounding cloud computing. The clear cut distinction between data controllers and their helpers, the processors, on one hand and the data subjects on the other, is no longer an adequate model of personal data processing. Nor is the idea that data is processed for a single, or limited set of purposes. Data that is disclosed to friends is also used for targeted advertising, tailoring services etc. This makes the link between purposes and controllers opaque, even though, in theory at least, the links can be articulated. Territoriality of controllers also loses its significance when data moves from data centre to data centre and, most of the time, this is not important from the perspective of privacy protection. What matters is who decides what happens with data. The current way of bringing non-EU entities under EU jurisdiction (the cookie-equipment route) seems to me to be a way of bypassing the problem rather than a proper way to make non-EU data controllers responsible for their actions. Finally, I think phenomena such as web 2.0 and cloud computing make clear that the whole concept of personal data and what we purport to facilitate and protect requires reflection: and this is precisely what the Commission is currently doing in the revision of the DPD.

Bibliography

Article 29 Data Protection Working Party (2002). Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP 56). Adopted on 30 May 2002.

Article 29 Data Protection Working Party (2007). Opinion 4/2007 on the concept of personal data (WP 136). Adopted on 20 June 2007.

Article 29 Data Protection Working Party (2008). Opinion 1/2008 on data protection issues related to search engines (WP 148). Issued on 4 April 2008.

Article 29 Data Protection Working Party (2009). Opinion 5/2009 on online social networking (WP 163). Adopted on 12 June 2009.

Article 29 Data Protection Working Party (2010). Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169). Adopted on 16 February 2010.

CATTEDDU, Daniele; HOGBEN, Giles (Eds.) (2009). *Cloud Computing. Benefits, risks and recommendations for information security*. Heraklion: ENISA.

KUCZERAWY, Aleksandra (2010). "Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS". In: M. BEZZI et al. (Eds.). *Privacy and Identity Management for Life*. IFIP Advances in Information and Communication Technology. Boston: Springer. Pp. 75-85.

LEENES, Ronald (2008a). "Do They Know Me? Deconstructing Identifiability". *University of Ottawa Law & Technology Journal*. Vol. 4, iss. 1 & 2, pp. 135-61.

LEENES, Ronald (2008b). Protecting identity online: law and technology? – User-centric identity management as an indispensable tool for privacy protection. *International Journal of Intellectual Property Management*. Vol. 2, iss. 4, pp. 345-371.

MEIL, P.; GRANCE, T. (2009). Definición de *Cloud Computing* del NIST. Version 15, 10-07-09. Gaithersburg, MD: National Institute of Standards and Technology (NIST). <http://csrc.nist.gov/groups/SNS/cloud-computing/>

POULLET, Yves; VAN GYSEGHEM, Jean-Marc; MOINY, Jean-Phillipe; GÉRARD, Jacques; GAYREL, Claire (en prensa, 2011). "Data protection in the clouds". In: Serge GUTWIRTH; Yves POULLET; Paul DE HERT; Ronald LEENES (Eds.). *Computers, Privacy and Data Protection. An Element of Choice*. Dordrecht: Springer.

VAN GYSEGHEM, Jean-Marc; GÉRARD, Jacques; GAYREL, Claire; MOINY, Jean-Phillipe; POULLET, Yves (2010). *Cloud computing and its implications on data protection*. Namur: CRID. <http://www.crid.be/pdf/public/6471.pdf>

Recommended citation

LEENES, Ronald (2010). "Who Controls the Cloud?". In: "6th IDP Conference. Cloud Computing: Law and Politics in The Cloud" [online monograph]. *IDP. Revista de Internet, Derecho y Política*. No. 11. UOC. [Accessed: dd/mm/yy].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-leenes/n11-leenes-eng>

ISSN 1699-8154

About the author

Ronald Leenes
r.e.leenes@uvt.nl

Dr. Ronald Leenes is professor in Regulation by Technology at TILT, the Tilburg Institute for Law, Technology, and Society (Tilburg University). His primary research interests are privacy and identity management, regulation of, and by, technology. He is also involved in research in ID fraud, biometrics and Online Dispute Resolution.

Tilburg Institute for Law, Technology, and Society
Tilburg University
Warandelaan 2
5037 AB Tilburg, The Netherlands