CHAPTER 7. Risks and compliance in cloud computing environments – views from Europe and the USA

a. Introduction – scope of this chapter

The aim of this chapter is to continue the analysis on the fundamental issues that any piece of regulation aiming to regulate legal issues arising out of the use of cloud computing should provide answers for. After having gone over the issues of accountability and jurisdiction, we will now look into defining what are the main risks posed by the cloud as a technology, to the extent that it is possible to make such an assessment being based on the current state-of-the-art of cloud computing technology. Additionally, the main compliance policies are discussed, in order to be assessed for sufficiency and compatibility with the main legal norms and values prevailing in the discussion for the construction of a working regulatory framework for the cloud.

PART I: THE RISKS ASSOCIATED WITH CLOUD COMPUTING

a. Privacy issues raised on the cloud: existent for all kinds of data across all types of cloud networks

Cloud architecture poses by nature implications for the privacy of all different kinds of information hosted on cloud networks[695]. Be it personal, business or governmental information, in order to capitalize on efficiency and maximize the economies of scale, cloud ecosystems usually adopt technological concepts that stand on the axis between security and privacy[696]. And although piling up on security safeguards is one way to deal with the insecurities that come along with the cloud, privacy issues cannot

695 Refer also to Chapter 2.

696 Robert Gellman, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, available at: https://www.worldprivacyforum.org/2011/11/resource-page-cloud-privacy/ (20 April 2015.)

and should not be disregarded when trying to grasp the bigger picture and construct an all-inclusive regulatory scheme for cloud computing[697].

A crucial factor determining the privacy and confidentiality risks a cloud computing user faces are the terms of service and privacy policy established by the cloud provider in the predesigned service agreement that the customer is required to sign. Several efforts have been made to present in a collective manner the different versions of service agreements proposed by various cloud computing service providers. Nevertheless, it is true that we are far from achieving an adequate level of awareness among users about the varying versions of contractual clauses available on the market for the kind of cloud service they are looking for[698]. Nor would it of course be legally sound to force the market to adapt to one specific prototype for conditions for offering cloud services[699]; that would be an undesirable market intervention, only paving the way to illegal disruption. As a result, this diversification of terms of service is here to stay and from a market point of view, it will not go away any time soon. Consequently, the challenges to privacy of users' data depending on the cloud provider they engage with are a challenge that needs to be adequately tackled with, in the context of a regulatory regime for the cloud.

For certain types of information and specific categories of cloud computing users, privacy and confidentiality rights, obligations, and status may change when a user discloses information to a cloud provider[700]. This is, for example, the case when a government authority switches to cloud computing in order to cover its data storage needs or when the same type of body deserts, mostly for reasons of economies of scale, its privately owned and maintained storage facilities over hosting and storage services from one of the private suppliers on the market (differentiation of privacy status within the same jurisdiction). Similarly, a change in the privacy status emerges in the example of data referring to health records when such archives migrate from cloud computing facilities located in one specific jurisdiction to different servers somewhere else in the world (differentiation of privacy status as a result of changing jurisdiction).

---

697 Paul Schwartz, *Information Privacy in the Cloud*, 161 University of Pennsylvania law review 1623–1662 (2013.)
698 Robert Gellman (note 696).
699 *Id.*
700 *Id.*

Disclosure and remote storage may have adverse consequences for the legal status or protection of personal or business information[701]. For instance, there are clear differences between the handling of data referring to tax and income information of citizens or businesses in Europe and the US. Similarly, business-owned data are under clearly varying protection between EU and US law[702].

As it has already been demonstrated[703], the location of information in the cloud may also have significant effects on the privacy and confidentiality protections of information and on the privacy obligations of those who process or store the information as well as on how the upholding of these obligations is legally evaluated. Additionally, co-existing jurisdiction laws may result in information in the cloud having more than one legal location at the same time, with differing legal consequences[704]. Privacy of data on the cloud can also be put in question due to different laws that may oblige a cloud provider to examine user records for evidence of criminal activity and other matters. And these are just very few examples of the differences in treatment data on the cloud may receive depending on which laws a certain cloud facility, network controller, cloud service provider or data processor is subject to.

In summary, legal uncertainties make it difficult in various ways to assess the status of information in the cloud as well as the privacy and confidentiality protections available to users.

The above risks to privacy are generally more likely to occur in the context of the US legal system[705]. The following are some characteristic instances of US laws which set fertile ground for undermined privacy of data stored on or transferred via cloud computing networks, certainly when compared to the prevailing legal thinking in Europe:

---

701 Robert Gellman (note 696); Clare Sullivan, *Protecting digital identity in the cloud: Regulating cross border data disclosure*, 30 Computer Law & Security Review 137–152 (2014.)

702 See Chapter 3.

703 See Chapter 6.

704 Id.

705 Robert Gellman (note 696).

i. United States v. Miller

In this cornerstone case brought before the US Supreme Court in 1976, Mitch Miller[706] was charged with carrying alcohol distilling equipment and whiskey on which liquor tax had not been paid. The Bureau of Alcohol, Tobacco, and Firearms (ATF) issued subpoenas to two of Mr. Miller's banks, The Citizens & Southern National Bank of Warner Robins and the Bank of Byron requesting records of Miller's accounts. The banks complied with the subpoenas, and the evidence was used during Miller's trial in the United States District Court for the Middle District of Georgia. Miller was convicted and appealed his conviction alleging that his Fourth Amendment rights were violated. The United States Court of Appeals for the Fifth Circuit ruled in his favor. The case was then brought before the US Supreme Court with the question whether Miller's bank records had been illegally seized in violation of the Fourth Amendment. The Court answered negatively; in a 6-3 opinion, it reversed the Fifth Circuit and held that Miller had no right to privacy in his bank records. Writing for the majority, Justice Lewis F. Powell asserted that the "documents subpoenaed are not [Miller's] 'private papers',"[707] but instead, part of the bank's business records. Consistent with Hoffa v. United States[708], the Court found that Miller's rights were not violated when a third party – his bank – transmitted information that he had entrusted them with to the government.

While the prevailing aspects of the specific case are arguably unique to banking, the decision brought out by the US Supreme Court in Miller stands generally for the proposition that an individual's personal record held by a third party does not have the same constitutional privacy protection as the one that applies to the same record when this is held by the individual. From a privacy perspective, this proposition and the doctrine it has fostered are unsettling because of the volume of personal information necessarily held by third parties today[709]. In the cloud context, cloud service providers could very likely be regarded as third parties in the meaning of United States v. Miller.

706 United States v. Miller, 425 US 435 (1976).
707 Id.
708 Hoffa v. United States, 385 US 293 (1966).
709 *Id.*

ii. The Electronic Communications Privacy Act (ECPA) – a step ahead but obscurity lingers

The Electronic Communications Privacy Act (ECPA)[710] is legislation dating back to 1986 and was enacted by the United States Congress with the aim of extending government restrictions on wire taps from telephone calls to the field of transmissions of electronic data by computer as well as adding new provisions prohibiting access to stored electronic communications.

In an electronic environment, the ECPA provides certain protections against government access to electronic mail and other types of computer records held by third parties (e.g., Internet service providers or cloud service providers). ECPA was an attempt to bring the constitutional and statutory protections against the wiretapping of telephonic communications into the computer age. Since its enactment and all the more so nowadays, ECPA is generally regarded as a difficult law to understand and apply[711]; on the one hand, it is an old law that relies and was inspired by a model of electronic mail and Internet activity that is generations behind current practice and technology. It is commonly agreed that ECPA is significantly out-of-date, at least in certain aspects[712]. Nevertheless, it reflects a legislative recognition that some Internet activities do merit protection from the Miller doctrine that there is no reasonable expectation of privacy in records maintained by third parties. The difficulty with ECPA, however, is figuring out what those protections apply to and when.

710 ECPA (Pub. L. No. 99-508, 100 Stat. 1848 (Oct. 21, 1986), codified at 18 U.S.C. §§ 2510-22, 2701-11, 3121-26) was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic communications. Since its enactment, the ECPA has been amended by the Communications Assistance for Law Enforcement Act (CALEA) of 1994, the USA PATRIOT Act (2001), the USA PATRIOT reauthorization acts (2006), and the FISA Amendments Act (2008).

711 *Id.*

712 *Id.*

iii. The USA PATRIOT Act

The USA PATRIOT Act[713] includes provisions allowing the FBI to access virtually any business record. Although a court order is required, the FBI's authority under the USA PATRIOT Act is sufficient to extend also to a record maintained by a cloud provider. The authorities granted by the USA PATRIOT Act weaken certain privacy protections from the ECPA, and they generally allowed for an expansion of the government's ability to compel disclosure[714]. What is more, anyone who receives an order to disclose information under a provision of this Act is highly limited in their ability to disclose that they have received such an order[715]. Consequently, a user who provided records to a cloud provider for storage or processing is highly unlikely to know that the government obtained those records if this has been effected under a provision of the USA PATRIOT Act.

iv. The HIPAA and compelled disclosures

Potential threats to privacy currently exist for cloud services and the use of them under US law not only in relation to demands from the central government or other government agencies, but also with regard to demands that are permissible by law from private parties. One typical such example

713 The USA PATRIOT Act (note 215) was signed into law by President George W. Bush on October 26, 2001. Its title is in fact a ten-letter acronym (U.S.A. P.A.T.R.I.O.T.) that stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001". On May 26, 2011, President Barack Obama signed the PATRIOT Sunsets Extension Act of 2011, a four-year extension of three key provisions in the USA PATRIOT Act: roving wiretaps, searches of business records, and conducting surveillance of "lone wolves"—individuals suspected of terrorist-related activities not linked to terrorist groups. Resulting from a lack of Congressional approval, parts of the Patriot Act expired on June 1, 2015. However, with the enactment of the USA Freedom Act on June 2, 2015 the expired parts were restored and renewed through 2019. Nevertheless, Section 215 of the law was amended to stop the National Security Agency (NSA) from continuing its mass phone data collection program. Instead, phone companies are nowadays obliged to retain the relevant data and the NSA can obtain information about targeted individuals with permission from a federal court.

714 *Id.*

715 *Id.*

is the HIPAA[716] Privacy Rule, part of the respective HIPAA Act, which imposes some limits on compelled disclosures of health data that are provided for by this law. In detail, a legal demand by a private party to a cloud provider for disclosure of protected health information has to follow the procedures set out in the rule governing judicial and administrative proceedings. In general, the rule stipulates that anyone seeking access to information constituting part of a patient's health record via a court order, subpoena, discovery request, or the like must notify the patient, who has an opportunity to object to the disclosure. The said necessity under HIPAA means that a cloud provider should duly notify prospective customers that it maintains patient records to which specific procedures apply if the provider receives an order for disclosure of a record that is held (stored or processed) on behalf of an entity making use of the provider's services[717]. While the burden of those procedures falls on the person seeking the records, problems of control and compliance have never ceased to exist also on the part of providers.

While HIPAA provides for such a process of notification as a safeguard to users' privacy, other personal information shared by a business with a cloud provider will most likely receive less detailed treatment with regard to an obligation for disclosure by the provider. It goes without saying that when a cloud provider allows anyone to use its resources without any contractual or other prearrangement, the provider may have little or no knowledge about the information that a user puts on the cloud. If a cloud provider is not legally obliged to consult with the user, is not motivated to consult with the user, or is actively prevented from notifying the user, any subsequent disclosure by means of a court order or subpoena may have undesirable consequences for the user or for the ultimate data subject.

716 HIPAA (Health Insurance Portability and Accountability Act), Pub.L. 104–191, 110 Stat. 1936, was passed by Congress in 1996. It is the federal law that establishes standards for the privacy and security of health information, as well as standards for electronic data interchange (EDI) of health information.

717 *Id.*

v. The Fair Credit Reporting Act

The Fair Credit Reporting Act[718] (FCRA) is one more example of US legislation that nurtures potential undermining for users' privacy on the cloud. The Act imposes limits on the use of credit reports specifically to what is defined as a 'permissible purpose' by it[719]. If a creditor stores a credit report with a cloud provider and a third party obtains the report from the cloud provider, the legal limit on use of it could be violated.

A violation of the FCRA may also occur if the cloud provider uses the stored credit report for an improper purpose. Despite imposing a restriction on uses of credit reports, the FCRA does not have a mandatory procedure comparable to the one articulated by HIPAA that would require informing a cloud provider that it has information subject to disclosure limits. As a result, a crediting institution that stores records with a cloud provider may unexpectedly confront legal problems due to this vagueness in law.

The above examples are demonstrative of how privacy can be put under question and should not be taken for granted in today's cloud cased environments under the laws that currently regulate them. In previous parts of this research, we have already explored similar pathologies for privacy under the current EU legislation[720]. In conclusion, it should be admitted that differences in legal culture and traditions do not result in 'right or wrong' situations, i.e. conditions where one legal order is right and the other wrong about privacy. On the contrary, conditions undermining privacy may be traced in both cases. Therefore, convergence and the promotion of a minimum common ground of understanding becomes necessary for a sound governance of cloud computing technology and its uses.

718 The Fair Credit Reporting Act (FCRA), title VI of Pub.L. 91–508, 84 Stat. 1114, is a piece of U.S. Federal Government legislation enacted to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. It was originally passed in 1970 and is enforced by the US Federal Trade Commission, the Consumer Financial Protection Bureau and private litigants.

719 *Id.*

720 See Chapter 4.

b. Threats to privacy means threats to security: the two prominent issues that go hand in hand in cloud computing environments

Threats to privacy in cloud environments are usually followed or set fertile ground for subsequent threats to security as well. In fact, the best angle from which privacy and security concerns that can arise when moving to the cloud are best observed and, thus, profoundly understood is from a risk–based perspective[721]. On further articulation, privacy and security risks on the cloud can be divided into operational, regulatory and compliance risks[722].

As it has already been extensively argued[723] many of the privacy and security concerns raised in the context of cloud computing are a direct consequence of the nature of the cloud; particularly in the early years of cloud adoption, its benefits had been invariably presented in terms of cost reduction, thus overlooking some of the inherent risks the new technology was bringing along, which have been left until now insufficiently addressed from a regulatory and, at times, also from a technological point of view. According to this angle, the cloud achieves its renowned economies of scale, that have actually enabled it to rise so quickly as a ruling technological standard in the field of IT services, thanks to a transformation of the nature of IT provision from specific, internally hosted and managed IT resources to commodity hardware and software platforms hosted outside the organizational boundary[724]. As it is known, in order to achieve this low-cost offering, cloud providers may switch customers' data and processes from one hardware facility to another; it is precisely this switching that nourishes some of the most common privacy and security issues with regard to the cloud.

The risks posed to privacy and security are relevant not only to cloud customers but also to cloud service providers. And this is not merely due to marketing or customer satisfaction reasons. As it has already become evident and will further be demonstrated on the course of this study, any loophole left in the overall structure of cloud computing environments and

721 A. E. Whitley, P. L. Willcocks & W. Venters (note 119).
722 Webster, J., & Watson, R. T., *Analyzing the past to prepare for the future: Writing a literature review.*, 26 MIS quarterly 13–23 (2002.)
723 See also Chapters 2 and 3.
724 Willcocks, Leslie P., Venters, Will and Whitley, Edgar A. (note 111).

the regulation thereof poses serious legal questions as well, apart from liabilities of any other nature.

Consequently, from a cloud computing customer's point of view, be it an average private customer or a big enterprise user or even an entity belonging to the wider administrative and government sector, the first set of questions relating to concerns that the use of the cloud is bringing forward are:

- Users wish to receive guarantees that their data and processes are not accessible to staff working for the cloud service provider or to other users running their processes on the same hardware environment as them[725].
- Users wish to have reassurances that, when the use of the hardware by them comes to an end (either because the specific service can no longer meet their demands, because the cloud hardware is decommissioned or because the cloud provider relocates the customer's services to other, cheaper computing resources) any data stored on that hardware is irreversibly removed. In the event the cloud provider is bound by any legal provision to retain data, users wish to have guarantees that their data will remain accessible to them during the retention period[726].
- Specifically in the case of cloud providers hosting mission critical services, users demand reassurances regarding the effectiveness of the cloud provider's disaster recovery plans[727].
- One of the greatest issues for cloud users, as it usually happens with every market growing in an accelerated manner, is the risk of attempts, on behalf of service providers, to lock–in the customer by methods, such as the use of non–standard hardware configurations or by making it impractical for them to transfer their data and processes to another provider[728].
- It is very typical for cloud facilities to host in their resources multiple service providers' data and processes. Sharing a storage facility with multiple other service providers can have unintended consequences that cannot be easily measured in advance. For example, one unpre-

725 A. E. Whitley, P. L. Willcocks & W. Venters (note 119).
726 Willcocks, Leslie P., Venters, Will and Whitley, Edgar A. (note 111).
727 DER HESSISCHE DATENSCHUTZBEAUFTRAGTE, Key data protection points for the trilogue on the General Data Protection Regulation (2015.)
728 Siani Pearson, Taking account of privacy when designing cloud computing services (2009.)

dictable consequence of Amazon and DynDNS hosting WikiLeaks was that these services were targeted by hackers with consequent adverse effects on other users of their services[729].

From a cloud provider's point of view, some of the major privacy and security concerns raised by cloud computing and the way it is technically built are:

– In an effort to respond to their users' worries, cloud providers apply different levels of staff accreditation to demonstrate to their customers that their staff will not misuse the data held on their cloud hardware. The number of different levels of staff accreditation and the distinctive features of each one of them has constantly been a matter of concern among cloud service providers[730].
– In response to the demand for safeguard mechanisms that permit unequivocal deletion of data hosted on a cloud facility after a user's quitting of the use of that facility, cloud providers look into the possibilities for developing such tools for data–wiping processes. In the context of such plans, cloud providers have to deal also with the issue of the cost, in capital and resources, for making these tools available to their customers, as well as whether it makes sense to give these options as standard tools to all users or offer them on a premium basis[731].
– A major challenge for cloud providers is also to put in place recovery mechanisms that will help contain the damage caused as a result of a major outage of service[732].
– Last but not least, cloud providers face the challenge to balance between offering commodity products on the basis of price and service quality and offering distinctive capabilities which might raise customer concerns about lock-in[733].

The privacy and security concerns described above are obviously common to users and suppliers of cloud computing services in both the EU and the US. However, the fundamentally different approaches the two jurisdictions take on privacy result in fragmented responses to common issues. While in the EU privacy is regarded as a fundamental human right, in the US it is viewed as a demand that businesses need to meet in order to pre-

729 A. E. Whitley, P. L. Willcocks & W. Venters (note 119).
730 Siani Pearson (note 728).
731 Francesca Musiani & Internet Policy Review (note 660).
732 Siani Pearson (note 728).
733 *Id.*

vent specific, serious risks of economic harm that may result from misuses of sensitive personal data[734]. These divergent approaches, however, work on the opposite direction of the tendency for more and more universal cloud services. Therefore, since cloud ecosystems and facilities are growing more and more unaffected of any kind of regional boundaries, an equally convergent mindset needs to be adopted towards setting up rules that will be based on shared principles and will create a minimum common understanding for tackling the risks rising out of the use of cloud computing.

c. Privacy risks posed by the cloud put into question cornerstone elements of information privacy laws

The architectural foundations of cloud computing technologies, along with the questions it raises regarding privacy and security of data and processes hosted in cloud ecosystems, have all contributed in basic definitions of information privacy law being challenged. Legislation developed in Europe before cloud computing, which became so widely used in the field of IT and data processing, understood information privacy law as a body of legislation concerning the processing of personal data[735]. Yet, with the arrival of cloud questions have been raised as to the meaning of both "personal data" and the "processing" of that data"[736].

The decisive criterion for the application of privacy law in the European Union is the assessment of whether personal data are involved. As it has been already demonstrated[737], personal data under EU law is any information that refers to "identified or identifiable" persons[738]. More explicitly, the EU Data Protection Directive would define that "an identifiable person is one 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, physiological, mental, economic, cultural or social

734 Nancy J. King & V. T. Raja (note 245).
735 Gerrit Hornung, *Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework*, 26 Innovation: The European Journal of Social Science Research 181–196 (2013.)
736 Paul Schwartz (note 697).
737 See Chapter 4.
738 Directive 95/46/EC, art. 2(a) (note 143).

identity"[739]. As long as the information at hand refers to identified or identifiable persons, information privacy law applies. This approach has been transposed to the newly introduced Data Protection Regulation[740] as well.

Following this track, the GDPR goes one step further to offer more details in an overall effort of greater specificity, wherever possible, compared with the Directive. Under the Regulation, the definition of persons as "identified" or "who can be identified" (i.e. identifiable) brings to the forefront the critical concept of direct or indirect identification by "means reasonably likely to be used"[741]. In this matter, EU law has been heavily influenced by German law, which has since long held the "means reasonably likely to be used" as the key criterion in defining whether or not a piece of information is identifiable[742]. The Regulation also sets out some additional typology criteria that help to make the relevant analysis more concrete: in that sense, it is specified that identification may be effected "by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person"[743]. These additional details provide useful guidelines for the successful execution of the required assessment of whether some information refers to a specific person or not.

Looking into the United States and how the same issue is viewed under the American legal thinking, the decisive element there is whether a piece of information relates to an identified person[744]. Unlike the EU's proposed Regulation, which offers a central point of reference regarding how to reach this determination over specific data, in the US there is no universal test but rather a variety of them scattered around federal and state statutes and regulations for deciding when information relates to an identified person[745]. Overall, it can be noted that US law does not extend as far as identifiability in order to grant to specific information the quality of falling under information privacy law; as a general rule, the U.S. threshold approach

739 Id.
740 Regulation (EU) 2016/679, Art. 4(1) (note 25).
741 Regulation (EU) 2016/679, Preamb. 26 (note 25).
742 Anne Arendt, Ulrich Dammann & Spiros Simitis, Bundesdatenschutzgesetz (2011.)
743 Regulation (EU) 2016/679, Art. 4(1) (note 25).
744 Paul M. Schwartz & Daniel J. Solove (note 16).
745 Paul Schwartz (note 697).

for defining information as personal is reductionist when compared with the European Union's expansionist approach[746]. Under US law, personal information is typically found to be at stake only when the data under examination refers to a currently identified person[747]. Except for the points of difference, there are also similarities in the EU and U.S. legal approaches to determining the moment when information falls within the scope of information privacy law. Rather than drawing a fixed line between personal information and non-personal information, both legal systems establish a determination mechanism that depends on a number of factors, such as technology and corporate practices[748].

It is crucial to point out, however, that whether information becomes personal information in a networked environment depends on decisions made throughout the world, sometimes in real time. Consequently, it is getting increasingly difficult to decide a priori if certain kinds of cloud data processing have to be determined by privacy information law provisions or not[749]. This difficulty is all the more intensified with the ever-greater adoption of the cloud, which has managed to profoundly destabilize the regulatory approaches to personal information in the European Union and United States alike.

From the perspective of EU law, the cloud has increasingly been accepted as a "means reasonably likely to be used", thus being considered as responsible for making more information "identifiable" and, consequently, more extensively, if not entirely, falling under information privacy law. Yet, it should not be overlooked that identifiable information is not synonymous to identified information, while there are indeed instances of identifiable information which may never elevate into the status of identified information[750]. Furthermore, different risks are associated with the possible identification of data compared to information already related to an identified person[751]. Therefore, EU legislation needs to fine-tune itself in order to strike a balance between its expansionist protection approach regarding privacy and the necessary vital space cloud computing necessitates in order to flourish as a technology. At the same time, the US ap-

746 Paul M. Schwartz & Daniel J. Solove (note 16).
747 *Id.*
748 *Id.*
749 Paul M. Schwartz (note 157).
750 Paul Schwartz (note 697).
751 Ulrich Dammann & Spiros Simitis (note 169).

proach appears too narrow: certain information may only be identifiable and not identified, but even so it might bring with it a substantial risk of identification[752]. As a result, certain rearrangements are necessary for US law, as well, in order to live up to the elevated privacy risks posed for information in such a dynamic environment, as today's cloud-based internet.

d. The other side of the coin: how cloud computing's architectural advantages can turn into threats for privacy

Privacy is a key business risk and compliance issue and even more so in the field of IT. Given that it sits at the intersection among social norms, human rights and legal mandates, privacy has been a key comparative criterion for all kinds of IT providers and this also applies for those active in the field of cloud computing. Conforming to legal privacy requirements or meeting client privacy expectations with regard to personal identifiable information, requires from businesses offering cloud related services to demonstrate a firm level of supervision over such processes at all stages of the cloud computing cycle, from collection to destruction[753]. On the other hand, the cloud has been traditionally praised for its competitive advantages over its predecessors, namely its abilities to scale rapidly, in-house or through subcontractors, to store data remotely and to share services in a dynamic environment. However, these very advantages can also become disadvantages in the effort to maintain a level of privacy assurance sufficient to sustain confidence in users. In particular, the main insecurities raised by the cloud's sui generis architecture are:

– Due to outsourcing: The widely-used practice of outsourcing of data processing by nature raises governance and accountability questions[754]. In detail, the use of outsourcing makes it imperative to develop rules and processes which will permit to clarify at all times which party is responsible (statutorily or contractually) for upholding legal require-

752 Paul Schwartz (note 697).

753 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

754 ACM ed., Controlling data in the cloud: outsourcing computation without outsourcing control (2009); Heinz-Dieter Schmelling, *Motivation. Wie verhält sich die IT-Sicherheit zum IT-Outsourcing?*, 40 Datenschutz und Datensicherheit – DuD 635–639 (2016.)

ments regarding privacy, or to verify that appropriate data handling standards are set and followed[755]. In an effort to further uphold privacy, effective methods for auditing third-party compliance with privacy laws and standards are also needed. Such methods will help determine to what extent it is safe to further sub-contract processing, and to confirm the identities and bona fides of sub-contractors[756]. Extensive use of outsourcing also necessitates rules that will permit to allocate rights in the data that are transferred between data processors and their sub-contractors or that they will even settle other instances, such as whether and how such data are transferable to other third parties upon bankruptcy, takeover or merger of the entity that initially undertook the outsourcing[757].

– Due to offshoring[758]: Offshoring is another practice widely used by cloud service providers in their effort to maximize their competitive advantages and secure an even wider client base. At the same time, though, outsourcing of data processing increases risk factors and legal complexity. An indicative list of the complex issues that a cloud computing service which relies on outsourcing and offshoring can raise includes issues of jurisdiction, choice of law and enforcement[759]. A comprehensive cloud computing regulatory framework must include rules that will help settle these issues.
– Due to relying on virtualization: Cloud computing has been made possible largely thanks to the extensive use of virtualization[760]. However, sharing hardware, which is basically what virtualization is all about, carries along multiple security risks; among others, loss of control over data location or who has access to it at any given time. In fact, these insecurities will be even graver for certain types of data as a result of their nature[761]. For example, transactional data is a typical example of a byproduct with unclear ownership; when transferred or processed on

755 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).
756 *Id.*
757 ACM ed. (note 754).
758 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).
759 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119); Heinz-Dieter Schmelling (note 754).
760 For more see Chapters 2 and 8.
761 A. van Cleeff, W. Pieters & R. J. Wieringa (note 119).

virtualization based networks, it can be hard to define whose duty is at any given time during the data life cycle to protect it[762].

– Due to the autonomic elements of cloud computing technology: Given that technological processes on a cloud environment have been granted a degree of autonomy in decision making (as they, for example, have the possibility to automatically adapt service resources to meet continuously varying needs of customers and service providers) it becomes more and more challenging for enterprises to maintain consistent security standards or to provide appropriate business continuity and backup[763]. This is a natural consequence of the fact that it may not be continuously possible to determine in real time and with specificity where data processing will take or is taking place within the cloud.

All these risks make it clear that in a regulatory framework specifically developed for the cloud, rules will need to take into account the cloud's architectural specialties and offer constructive answers regarding them. Some proposals about how this could be achieved on the management and governance of the cloud level have already been presented in the introduction of accountability as a suitable managing framework for the cloud[764].

e. The affluence of consumer data on cloud computing and particular threats to them because of the cloud's specificities

Cloud computing is a high-end technology which has rapidly grown to be utilized for managing a wide range of commonplace information. One could persuasively argue that the cloud today is basically the internet, although, as it has been already explained, these two notions are not identical[765]. A logical outcome of this widespread deployment of cloud computing has been that the cloud is the vessel that hosts a staggering affluence of data and information from billions of common users[766]. A lot of this data may seem rudimentary from a wider perspective yet for individual users they constitute their very personal and sensitive information.

---

762 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

763 *Id.*

764 See Chapter 6.

765 See Chapter 2.

766 Paul Schwartz (note 697).

The need to host or process this exponentially growing data has fueled the creation and use of massive cloud data centers, and cloud service providers such as Amazon have already invested enormous amounts in building and operating large data centers that provide a seemingly "infinite capacity" of computing resources to their clients[767]. All these facilities and the countless different types of information that is hosted on them pose certain risks apart from the ones we have already discussed in relation to how the life cycle of data evolves on the cloud computing network. Firstly, energy grids that power these data centers may be subject to attacks, which could be lengthy. Such power outages or other data center hardware-related disasters could have a significant impact on the business continuity of service providers[768]. If a provider's disaster recovery procedures for its data centers are inadequate, this sensitive data described beforehand run the risk of being lost or irreparably damaged. Secondly, current laws do not necessitate from cloud service providers to disclose sufficient information about the security policies and disaster recovery procedures they have designed in relation to their data center operations[769].

From a data architectural point of view, cloud service providers use certain data management practices which also raise concerns regarding the integrity and safety of consumer data and call for concrete regulatory rules that will moderate such risks in the context of a specific set of cloud computing laws[770]. Data commingling[771] is the first important such risk and it occurs when different items or kinds of data are stored in such a manner that they become commonly accessible while they are supposed to remain separated. In a cloud environment, this can very easily occur where different customer data sits on the same server presenting a continuous security vulnerability. The reason why cloud service providers choose to store data from different clients in the same data files is, as expected, the wish for optimal utilization of resources, especially if different cloud users concur-

767 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

768 *Id.*

769 W. Kuan Hon, Christopher Millard & Ian Walden, *The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, Part 1*, 1 International Data Privacy Law 211–228 (2011.)

770 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

771 M. Zhou, R. Zhang, W. Xie, W. Qian & A. Zhou (note 119).

rently use the same applications on the same cloud server[772]. It needs to be made clear that commingling in data is not only a matter of digital data colocation but it also refers to physical commingling.

The other data practice that poses risks on consumer data hosted on the cloud is data aggregation[773]. Aggregation practices raise significant challenges for protecting sensitive consumer data in cloud computing environments[774]. Public clouds, i.e. those where the great majority of cloud services nest, typically aggregate numerous clients' data into single files, and the latter actually share applications, processing power, and data storage space all at the same time[775]. A single instance of an unauthorized penetration into one cloud server facility that houses large volumes of data may provoke a massive compromise of sensitive data of multiple cloud users at the same time[776]. In a way to put in place countermeasures for this risk, it has been suggested that cloud users, primarily businesses, should be in a position to screen the cloud computing users with whom they share the same servers, applications, and data files to verify whether those other users have good reputations[777]. Also, in an effort to reduce the risk of data espionage, it is suggested that cloud users should be able to opt out of the commingling of their data with those from competitors[778]. However, these are only business choices or tools and are offered mainly as market incentives, hence, they cannot be held as standard practice neither can they be enforced by law.

Currently, on a statutory level, actors of the cloud market try to deal with these insecurities posed to consumer data with ad-hoc cloud service agreements. However, just as it has been proved that these are not an adequate answer to the problem of jurisdiction determination on the cloud[779],

---

772 *Id.*

773 Data aggregation is the process of transforming scattered data from numerous sources into a single new one. The objective of data aggregation is to combine sources together as such that the output is smaller than the input. This helps processing massive amounts of data in batch jobs and in real time.

774 Dawn Song, Elaine Shi, Ian Fischer & Umesh Shankar, *Cloud Data Protection for the Masses* Computer 39–45 (2012.)

775 *Id.*

776 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

777 Dawn Song, Elaine Shi, Ian Fischer & Umesh Shankar (note 774).

778 *Id.*

779 See also Chapter 6.

they cannot deal inclusively with the issue of risks to data integrity either. In fact, it is more often so that individual cloud users do not have enough gravitational significance to negotiate the terms of cloud service agreements, particularly when they use the services of large public cloud service providers such as Amazon, Microsoft, Dropbox or Google[780]; in all these cases, there is a wide disparity in bargaining power between the parties which makes the chances to achieve a negotiated service agreement highly unrealistic due to lack of adequate bargaining power in this context[781].

In conclusion, the cloud as an industry is mainly footed by billions of plain private users who entrust with cloud service providers a great variety of their personal consumer data under pre-negotiated terms and conditions. All these clients lack the negotiating capacity to force the companies from which they are supplied with their computational needs to offer them contractual agreements with all the reassurances and safeguards that would allow them to feel secure about their data. Therefore, it is imperative need that a comprehensive cloud computing regulatory regime is put in place, which will set a level playing field for cloud users and service providers alike.

f. Reviewing security, privacy and trust issues on the cloud from an EU perspective

Having systematically examined the main points of concern regarding security, privacy and trust issues in cloud computing environments from a technical viewpoint and also through the angle of US law, this part of this study concludes with some observations regarding these issues from a European perspective. For starters, it is worth clarifying how EU legal thinking defines the main threats raised by cloud environments:

– Under the EU doctrine, security in the cloud concerns the confidentiality, availability and integrity of data or information[782]. Security as a

780 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).

781 Jack L. Goldsmith & Tim Wu (note 535).

782 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275). Kirstin Brennscheidt (note 119).

cloud necessity, may also include authentication and non-repudiation[783].

– Privacy refers to the expression of or adherence to various legal and non-legal norms regarding the right to private life. In the European context, ensuring privacy in the cloud has until today been understood as compliance with the European Data protection Directive[784] and since May 2018 with the respective Regulation. The main traits the concept of privacy in the cloud bears under the relevant tradition in EU law can be summarized down to these principles: consent, purpose restriction, legitimacy, transparency, data security and data subject participation[785].
– Trust is the concept encompassing the assurance and confidence that people, data, entities, information or processes will function or behave in expected ways[786]. The way trust in the cloud is interpreted as an idea under EU law is broken down to several different genres, i.e. trust from human to human, machine to machine (for example, handshake protocols negotiated within certain protocols[787]), human to machine (e.g., when a consumer reviews a digital signature advisory notice on a website[788]) or machine to human (e.g., when a system relies on user input and instructions without further verification to execute a process[789]). From a more thorough perspective, trust should be regarded as the logical consequence of progress towards achieving the broader security or privacy objectives the cloud industry has imposed on itself as essential.

Given the way these terms are interpreted in European legal thinking and the generally stricter protection that EU law grants to cloud related matters than US law, cloud computing raises serious challenges also for EU legislators. In fact, a new EU law aimed at regulating the cloud has to deal not only with the task of providing updated answers to commonly known IT problems as these are now readapted in light of cloud technologies but also to ensure that these answers will be fit for the market and technologi-

783 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).
784 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275).
785 See also Chapter 4.
786 Siani Pearson & Nick Wainwright (note 645).
787 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).
788 *Id.*
789 *Id.*

cal standards set out by cloud computing. Indeed, a great share of experts on the EU cloud services market have expressed the opinion that certain aspects of European data protection law (notably the rigid controller-processor model and the reliance on geographic location of data processing as an important factor in determining applicable rules) lead to substantial difficulties in practice[790]. Given that these understandings on which existing EU laws with which the cloud is attempted to be regulated have largely been rendered obsolete or unimportant by cloud technologies, a profoundly different approach is urgently needed.

What is also important to point out is the fact that, despite the strict rules regarding data protection, in practice there appears to be a substantial degree of poor compliance with them, especially in relation to transfers to third countries or data subject rights[791]. Both these topics merit careful analysis and consistent and clear responses in the context of a body of regulation dedicated to efficient governance of the cloud. Even in areas of data where more restrictive regulatory frameworks are in force, such as sensitive data mainly from health and financial industries, just adding extra impediments to data migrations or requiring that such data be processed only locally are not adequate measures to alleviate risks related to them[792].

Given the prevailing legal doctrine regarding IT technologies and the data tasks effectuated through them, the essential elements of an effective regulatory regime for the cloud should be transparency, availability and accountability. Transparency is an important element in the struggle to meet security, privacy or trust obligations, since it brings to the forefront the (contractual) will of all cloud actors (be them users, service providers, inspecting authorities etc.) to fulfil the globally accepted privacy principles that will make up for a sound and secure cloud environment[793]. Availability arises as a prerequisite since in a sound governance framework for the cloud availability for reporting and inspection of cloud actors is of

790 Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri (note 275).

791 W. Kuan Hon & Christopher Millard, *Data Export in Cloud Computing*. *How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4*, 9 SCRIPT-ed (2011.)

792 *Id.*

793 Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Chris Hanson, James Hendler, Lalana Kagal, Deborah L. McGuinness, Gerald Jay Sussman & K. Krasnow Waterman (note 21).

prime importance as an assurance for application of the commonly accepted privacy and security requirements[794]. Finally, accountability, as it has already been demonstrated[795], is an important factor arising directly from one of the main legal challenges with regard to cloud computing: namely that commitments from parties to the cloud life cycle must be clear and enforceable in practice[796]. This, in consequence, stimulates trust throughout the cloud cycle and further intensifies the bonds between providers and users of cloud services[797].

In summary, it has become evident from the discourse into the issue of risks related to cloud computing that the legal and, hitherto, the contractual framework for the cloud needs to become sufficiently stable and comprehensive to promote the trustworthiness of the legal relationships that are created among actors of the cloud life cycle[798]. At the same time, this requirement for trust and continuous accountability needs to be reconciled with the inherent flexibility of the cloud computing architecture[799]. In practice, this can only be achieved by ensuring that the rights, responsibilities and liabilities of each actor are clearly outlined, and that the expectations from each link in the cloud chain are at all times transparent and adequately ensured. If these conditions are met, then compliance (and accountability) become more realistic and lead to a viable and, simultaneously, trustworthy governing scheme for cloud computing.

PART II: CLOUD COMPLIANCE

a. Introductory remarks on the concept of 'cloud compliance'

Cloud compliance is the general principle that cloud-delivered systems must be compliant with standards that the cloud users face[800]. In other words, a cloud network and the providers of it or the services that are

794 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).
795 IEEE ed. (note 681).
796 Centre for Information Policy Leadership (note 592).
797 Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese & Paul P. Hopkins (note 119).
798 *Id.*
799 Liang-Jie Zhang & Qun Zhou (note 96).
800 Siani Pearson (note 728).

made possible thanks to it, need to live up to a series of expectations that the users of this network have in order to regard the network as a secure, safe and trustworthy one. Having gone through the overview of the perils that cloud computing might entail for the data users entrust it with, it has been made clear that effectively dealing with these risks is not just a regulatory matter but also an issue of credibility. Consequently, cloud compliance is for owners, controllers and service providers of a cloud network the litmus test in their relationship with cloud users as is accountability in their relation to regulatory authorities inspecting the overall cloud industry. Just as a cloud ecosystem has to meet specific standards set by its supervising public authorities to get the green light and be lawfully commercialized, it also needs to meet the same approval in the eyes of its actual users. After all, the risks that an effective body of law governing the cloud will try to keep under control or even resolve are the worries that users of cloud computing need to be reassured about. In conclusion, analyzing what cloud compliance constitutes of and discussing how these necessities will be pursued by an effective regulatory framework for the cloud is as important as highlighting how public authorities need and should inspect such a heavily customer-oriented industry.

b. Effective regulation of technology: the need to define policy tools and policy actors

Lawrence Lessig[801] had already since the 1990s put forward the regulation of privacy as 'an example of law taming code' in order to uphold expectations of users of IT technologies: in Lessig's doctrine, the state as an actor has the discretionary power to impose changes on code in order to increase the ability of the individual to exercise privacy choices[802]. This regulatory approach, involving the Platform for Privacy Preferences (P3P)[803], is fabricated upon the conception of privacy as a property

801 L. Lessig (note 504).

802 *Id.*

803 The Platform for Privacy Preferences Project (P3P) is a protocol permitting to websites to declare their intended use of information they collect from web browser users. It was developed with the aim of giving users more control of their personal information when browsing. It was officially launched in 2002 but there had been only limited implementations of it mainly due to its difficulty and lack of value.

right[804], in which the giving (or withholding) of consent is the cornerstone for protecting privacy. According to this predicament, the need for collective action by the state in order to enable individuals to control their own privacy by ensuring the availability of respective tools that will allow them to do so, is of prime significance for a well-functioning and soundly-regulated IT environment. It also constitutes an exemplary pattern of interaction among different constituents playing a role in the IT market.

Generally, a doctrine like this, which makes provision for specific policies and tools that enable private parties to have an actual say in how their right to privacy is handled, fits more comfortably in regulatory environments such as that of the USA, where political and business environments have shown a considerable resistance to more direct legislative solutions, such as non-consumerist, human rights-based conceptions of privacy, and, as a result, the range of alternative regulatory solutions has traditionally been restricted. However, at least as the prevailing legal thinking has been until now, such a doctrine mostly contrasts with the approach of European countries and the European Union. As it has been previously explained in detail[805], in the EU legal doctrine so far has been promoting more active roles for collective rather than individual actors, such as regulatory agencies. These have been the entities to play – in principle, at least – the key parts in the regulatory mechanisms for governing IT technologies and the markets dependent on them by executing the powers entrusted to them to implement legislation. Consequently, so far European law vests the main protective initiatives for privacy to state actors rather than individual citizens or consumers, or technological mechanisms.

In mid-2000s, when the revolution of cloud computing was still very nascent but indications about the cloud's potential were already growing, Murray's[806] doctrine of 'cyberspace regulation' was introduced in academic discourse putting emphasis on the need to identify distinct actors active within multi-level regulatory regimes[807]. Presenting his doctrine on an abstract level, Murray put forward an illustrative matrix to conceptualize multi-dimensional regulatory fields, i.e. fields of regulation with multi-

804 Charles D. Raab & Paul de Hert, *The Regulation of Technology: Policy Tools and Policy Actors* TILT Law & Technology Working Paper Series (2007.)

805 See Chpaters 2 and 3.

806 Andrew Murray, The regulation of cyberspace. Control in the online environment (2007.)

807 *Id.*

ple actors carrying some type of regulatory capacity for specific actions[808]. This conception was then tested against actual regulatory case-studies and led Murray to argue against static 'command and control' regulatory models in fields with actors spread through various levels. In the end, Murray concluded that in such multi-layered regulatory fields, regulation attempted exclusively via external interventions, typically manifested through law, is likely to be rather disruptive than effective. This is mainly so due to the fact that regulation produced entirely by actors on the superior levels of the system is grounded in insufficient understanding of the processes and interactions that are meant to be regulated. Instead, he argues in favor of a more dynamic, complementary and symbiotic approach, which acknowledges that regulators and regulates are not separate, and which relies on hybrid rule-making processes rather than instruments produced out of single-direction flows[809].

c. Incorporating users' privacy concerns into the rules governing design and deployment of cloud environments

Maintaining adequate levels of protection of data and privacy is not only a matter of legal importance but also crucial for responding to users' expectations in relation to the cloud. This challenge becomes even more complicated when the restrictions on cross-border data transfers are also to be upheld. This is not just an accountability issue, in the sense of self-disciplinary measures. As cloud services process users' data on machines that users do not own or operate themselves, serious privacy issues are raised which can undermine users' control and privacy options. However, privacy is a fundamental human right, enshrined in the United Nations Universal Declaration of Human Rights[810] and the European Convention on Human Rights[811]. Out of this basic privacy provisions come various special forms of privacy, including 'the right to be left alone'[812], the 'control of

808 *Id.*
809 *Id.*
810 The Universal Declaration of Human Rights, General Assembly resolution 217 A (1948), Art. 12.
811 The European Convention on Human Rights (ECHR) (note 343), Art. 8.
812 Siani Pearson (note 728).

information about ourselves'[813] or the newest concept of 'the right to be forgotten'[814]. These are all privacy manifestations which have been inspired by the way individuals have been interpreting their right to privacy over the years and they all play a crucial role in the way cloud technologies are or should be applied.

Apart from the concerns raised for privacy because of the very technological architecture of the cloud, another source of potential undermining effects for privacy on the cloud is that it is a dynamic environment, which facilitates, for instance, service interactions that can be created in a more dynamic way than traditional e-commerce scenarios[815]. In cloud enabled data paths, personal and sensitive data can move through an organization or cross organizational boundaries in various simultaneous trajectories. However, data remains at all times attributable to its original subjects, adequate protection of the information of which is as important as maintaining other aspects of legal compliance.

Apart from the multiple routes made available to data in their constant flow from one terminal point to another, cloud computing also makes possible for new services to be made available in the cloud, which come out of combining two or more individual services[816]: for instance, a cost-efficient 'pictures on demand' service could be made commercially available by combining a printing service with a cloud storage service. As this procedure of service combination grows into more layers, it typically leads to less and less control over aspects, such as the privacy of the data carried out for and due to the use of these services[817]. Additionally, while before the introduction of cloud computing such on-demand services involving data were made possible via traditional multi-party enterprise schemes, nowadays convergence happens on the services level, with the owner of provider of each service not even being necessarily aware of the combinations[818]. What is more, there might also be varying degrees of security, diverse privacy practices and controls in each of the component services. And given that, as every cloud service, they almost necessarily involve collection, storage or disclosure of personal and sensitive user data, poten-

813 *Id.*
814 Gerrit Hornung (note 735).
815 Siani Pearson (note 728).
816 *Id.*
817 Siani Pearson & George Yee (note 280).
818 Siani Pearson (note 728).

tial users need to receive adequate and persuasive reassurances before actually deciding to use them. It is precisely at this point, where cloud compliance comes to act as the catalyst that turns users' expectations into cloud service providers' self-discipline processes.

In light of the above observations on privacy expectations users have from cloud computing systems, the privacy concepts and principles that have prevailed may be summarized as follows[819]:

- Notice, openness and transparency: it is increasingly becoming a standard user expectation that cloud services which need to collect users' information duly inform them about the kind of information they collect, the ways in which they intend to use it, the amount of time that they intend to keep it, if it will be shared with any third parties, and the by-products of the further uses they intend to make of it. It is also expected that cloud service providers notify users before making any changes as to how the information is or will be used.
- Choice, consent and control: cloud services users expect to be given the freedom of choice whether they allow this information to be collected or not. Data subjects are also entitled to giving their consent to the collection, use and disclosure of their personally identifiable information.
- Scope/minimization: only information essential to fulfil the stated purpose should be collected or shared. The collection of data should be minimized to what is necessary for the service purpose.
- Access and accuracy: cloud services users expect at all times to be able to access the personal information service providers collect about them, to review what is being held about them, and to verify its accuracy.
- Security safeguards: users expect that safeguards are in place to prevent unauthorized access, disclosure, copying, use or modification of personally identifiable information
- Means to challenge compliance: users must have the possibility to challenge, ideally via official procedures, a provider's privacy processes.
- Limitation of purpose: users expect that their data will only be used for the purpose for which it was collected. This purpose is expected to be a clearly specified one. Data subjects are to be informed about the rea-

819 Refer also to Chapters 8, 9 and 10.

sons why their data is being collected and shared in advance or, at the latest, at the time of collection.
- Limited use – disclosure and retention: users expect that data will only be used or disclosed for the purpose for which it was collected and should only be disclosed to parties authorized to receive it. Additionally, personal data are expected to be aggregated or anonymized with suitable methods. Personal information should only be kept strictly for as long as necessary.
- Accountability: users expect that a provider has in place inspecting personnel that ensures that privacy policies and practices are followed at all times. Audit functions also play a crucial role towards monitoring data accesses and modifications.

As it easily becomes evident, the main expectations of users, which are the actual content of the concept of cloud compliance, are identical with respective elements of the suggested accountability scheme for the cloud[820]. This comes as no surprise given that, as it has been previously demonstrated, cloud compliance is the other side on the coin of sound cloud governance[821]. Much as providers try or should even be made to incorporate the above expectations already since the phase of preliminary design of their services, it may prove challenging to know exactly how their service will evolve. In conclusion, the flexible nature of cloud computing as technology necessitates respectively more adaptable design specifications. Consequently, the development of a regulatory framework for it comes also to challenge traditional thinking about legislation production[822]. In particular, as user requirements change, taking full advantage of the multiple possibilities offered by the cloud, so may functionality and privacy requirements[823]. On a regulatory level, this means that laws governing the cloud need to be produced via processes that will allow for more frequent and effective reassessment or that will aim at more generically formulated norms so that the gap between the legal and technological, as well as the service state-of-the-art can be shortened.

820 Siani Pearson & Andrew Charlesworth (note 585).
821 Refer to Chapter 5.
822 L. Lessig (note 504).
823 Siani Pearson & George Yee (note 280).

d. Pragmatic answers regarding the deployment of secure and privacy-proof cloud networks

The rate at which cloud computing is expanding across sub-domains of the IT sector proves its lasting nature as a technology. It has also been adequately demonstrated that trying to put geographical or other kinds of boundaries to the cloud is ineffective and out of touch with how cloud computing is being used in real life. Neither users nor cloud service providers will voluntarily quit from taking advantage of the full potential of cloud applications, which is decisively shaped by the universal nature of this technology. Therefore, also from the perspective of regulating how service providers should set up their services to make them compatible with cloud users' expectations, the focus should primarily be on restricting unauthorized access to intelligible data, rather than restricting data export[824] or other kinds of data processing that can be executed on the cloud. The current restrictions, via which data processing in the cloud is attempted to be regulated, should be replaced by requirements regarding accountability, transparency and security, i.e. with measures that will boost cloud compliance.

In fact, the preoccupation about setting boundaries is rather unnecessary if close attention is paid to how resources allocation in a cloud network actually works. While the popular view seems to be that in cloud computing data moves around the network continuously and almost randomly, making it virtually impossible to know where a specific bunch of data are located at any time, in practice this is often not so. In most cases, data are copied or replicated to different data centers, for business continuity/back-up purposes[825], rather than being constantly circulated through the networks storage facilities by being deleted from one data centre and re-created in another. Additionally, the primary copy of a set of data (e.g. data of a specific user inserted on a particular SaaS application) is at most times stored in the same data centre[826]. This typically is the one geographically closest to the user in question, for latency reasons (i.e. for achieving the optimum speed of access and response for the user[827]), even if it is also likely that they are stored in fragments distributed amongst different stor-

824 W. Kuan Hon & Christopher Millard (note 791).
825 *Id.*
826 *Id.*
827 *Id.*

age hardware within that data centre[828]. Consequently, regulating the cloud with a view to improving data allocation capabilities on cloud networks is not a real priority. If need be, the provider will most likely know where a user's data fragments are stored, on a data centre if not on equipment level.

Overall, it becomes evident that the regulatory focus regarding cloud computing needs to shift from where the data is or can be saved or processed to the intention (i.e. the purpose) for which it is saved or processed at any time by a specific actor of a cloud network. This approach towards cloud computing regulation through the teleological perspective will be thoroughly presented as the final outcome of this study[829].

e. Incentivizing privacy and security by encouraging the adoption of privacy enhancing technologies

In order to achieve a regime of effective data protection on the cloud, under the present and projected status quo of cloud technologies, legal instruments are not enough by themselves. A crucial tool in that direction will also be the availability of privacy enhancing technologies (PETs)[830]. It is beyond the scope of a legal research project to describe in detail the nature of PETs. Nevertheless, it should not fail our attention how PETs can assist in achieving optimum levels of privacy and security and why it is, therefore, important that their adoption be prescribed or, at least, encouraged by law[831].

The intrinsic and, largely, legitimate aim of service providers and users of cloud computing is the maximization of profit[832]. In this context, data protection could remain relevant as long as there is demand for it on the market. On the other hand, if such demand ceases or becomes minimal,

---

828 *Id.*

829 See Chapter 10.

830 Privacy enhancing technologies (PETs) is a generic term referring to a set of computer tools, applications and mechanisms which, integrated in online services or applications, or used in conjunction with such services or applications, enable online users to protect the privacy of their personally identifiable information (PII) which they have handed over to and is handled by such services or applications.

831 W. K. Hon, C. Millard & I. Walden (note 119).

832 See also Chapter 2.

privacy and the technologies making it possible may quickly become a mere cost driver or even end up being irrelevant in the design process because it neither causes nor reduces costs.

Therefore, in the context of an effective regulatory scheme for the cloud, it is crucial to emphasize the idea of service responsibility for service providers[833]. Rules can assist in that direction and have a relevant impact in several manners:

– by providing external incentives, such as binding requirements and restrictions or liability regulations[834].
– by exerting influence on intrinsic goals of service providers; in other words, by stimulating the market for PETs using data protection audits or quality certifications as means of pressure for providers to embrace these technologies[835].
– even by going as far as establishing guidelines for the participation of scholars and practitioners in interdisciplinary research that will be aimed at devising methods for privacy enhancing design of cloud-based services. The multi-faceted nature of the cloud means that, apart from legal experts, interdisciplinary research into the ever-enhanced privacy and security standards of cloud computing should also bring together experts from a wide range of areas, such as computer science, organization and management science, economics and political science.

In following parts of this study[836], it will be argued that PETs are no one-way solution, as far as regulatory handling of the cloud is concerned. Rather, they are just a tool that could offer greater assurance to consumers about the security of cloud systems. However, the philosophy behind PETs can already offer invaluable insight towards a thorough set of regulatory principles for the cloud which, coupled the expertise available from the technical front can ultimately lead to robust and efficient cloud regulation rules.

833 *Id.*
834 See also Chapter 6.
835 *Id.*
836 See Chapter 10.