
**International Journal of Cloud Computing**

ISSN online: 2043-9997 - ISSN print: 2043-9989
https://www.inderscience.com/ijcc

# Legal issues of consumer privacy protection in the cloud computing environment: analytic study in GDPR, and USA legislations

Alaeldin Alkhasawneh, Fawaz A. Khasawneh

**DOI:** 10.1504/IJCC.2023.10054987

**Article History:**

| | |
|---|---|
| Received: | 23 April 2019 |
| Last revised: | 16 February 2020 |
| Accepted: | 03 May 2020 |
| Published online: | 27 March 2023 |

# Legal issues of consumer privacy protection in the cloud computing environment: analytic study in GDPR, and USA legislations

Alaeldin Alkhasawneh*

Departement of Private Law,
Yarmouk University, Jordan
and
Department of Private Law,
UAEU University,
Sheik Khalifa Bin Zayed St,
Asharij – Abu Dhabi, United Arab Emirates
Email: Khasawneh_alaa@yahoo.com
*Corresponding author

Fawaz A. Khasawneh

Department of Software Engineering and IT,
University of Quebec – ETS,
1100 Rue Notre-Dame Ouest,
H3C 1K3, Montreal, QC, Canada
Email: fawaz.khasawneh.1@ens.etsmtl.ca

**Abstract:** Cloud computing services are considered among the most important services provided for companies due to the various benefits they confer. However, data privacy is a major concern for users, and laws covering this contain many contradictions and require improvement. This paper discusses the laws governing privacy issues in cloud computing, highlights missing components that could be added to laws, and proposes amendments to laws that may help create a better consumer experience, improved service, and increased protection for personal data. At the end of the paper, a set of recommendations is proposed for governments and private companies that would increase the responsibility held by cloud computing service providers in the event of failing to protect personal data from privacy invasion.

**Keywords:** consumer; privacy; cloud computing; legal protection.

**Reference** to this paper should be made as follows: Alkhasawneh, A. and Khasawneh, F.A. (2023) 'Legal issues of consumer privacy protection in the cloud computing environment: analytic study in GDPR, and USA legislations', *Int. J. Cloud Computing*, Vol. 12, No. 1, pp.40–62.

**Biographical notes:** Alaeldin Alkhasawneh received his PhD in Private Law in Civil Law from Universite de Reims Champagne, France in 2008. He is conducting research in fields such as private law, data privacy laws. Currently, he is an associate professor in the department of private law in United Arab Emirates University (UAEU).

Fawaz A. Khasawneh received his PhD in Electrical Engineering from University of Quebec (ETS), Canada, Master's degree in Electrical and Computer Engineering from Concordia University, Canada and Bachelor degree in Computer Engineering from Jordan University of Science and Technology (JUST). He is currently a Postdoctoral Fellow in University of Quebec, Canada in collaboration with Ericsson. His current research interests includes network function virtualisation, software defined network, network slicing and machine learning.

## 1 Introduction

The issue of privacy preservation is growing exponentially with the proliferation of cloud computing technology. This technology is offering an unprecedented elasticity in resources by providing savings in hardware and software costs. Cost effective large-scale service implementation is now possible because of cloud computing (Dorairaj and Kaliannan, 2015). However unlikely it may be, cloud service providers have the ability to intrude into the business' data and invade privacy because they have the control over the bottom layer of a software stack. To protect data integrity, cloud service providers may implement a virtualisation technique, which isolates the consumers from an internal intruder. In response, the consumer might incorporate encryption techniques to avoid exposure of data to attackers.

Cloud computing in this study refers to storing data in central storage spaces provided by third party vendors (cloud providers), who hold the responsibility of keeping data protected from attacks. Cloud providers commonly build a large storage facility containing hardware and software resources that are carefully designed to prevent abnormal conditions. Organisations subscribe to cloud services for holding their data in exchange for monthly charges. Facilities offered by cloud providers can be divided into: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In SaaS, organisations can use software solutions provided by the cloud providers. In PaaS, organisations are free to use the platform for the development of applications. In IaaS, the consumer can use the hardware and storage infrastructure offered by the cloud providers.

Cloud computing is increasingly significant in business environments that handle large amounts of data (Yang et al., 2017). It offers maintenance free, cost effective, and highly reliable storage facilities at the expense of nominal charges. In a highly competitive market setting, organisations can escape the financial and technical burden of maintaining local storage facilities and resort to cloud computing for better profitability and increased productivity. In a more agile and dynamic market setting, cloud computing can segregate information technology related concerns from core business operations and help management focus on goals and visions.

One of the major pitfalls of cloud computing is privacy. Keeping sensitive data in third-party storage always brings the integrity and confidentiality of the data into question. Being an internet-based technology, in which data and information are shared and transferred over the web, cloud services are highly vulnerable to all types of cyber-attack. To bolster privacy against these attacks, many techniques are adopted, which can include data encryption (Kanimozhi, 2019), access control, and the

implementation of disaster recovery plans. In addition to external attacks, the cloud environment is vulnerable to internal attack (Xiao and Xiao, 2013). Lack of control is another privacy concern since the cloud user has little control over the stored data, which can be altered by the provider.

The use of a highly sophisticated privacy protection technique can slow down the overall system (Tari et al., 2015). Furthermore, implementing a high-end privacy management scheme is a complex solution because of its scale and ubiquity. It is not possible to implement a plan to definitively protect the privacy of consumer data without compromising the advantages of the cloud. Some studies discuss privacy preservation issues (Li et al., 2017). However, some acts and laws issued by governments are considered an obstacle in ensuring the privacy of consumer data (Alrabaee et al., 2014).

The rest of the paper is organised as follows: Section 2 describes the existing the current laws applied to protect consumer data in cloud computing environment, then research gaps in these laws are discussed in Section 3, while in Section 4 policies adopted by different companies are introduced. Obligations of cloud computing service providers and liability in case of personal data privacy invasion are explained in Section 5 and finally a list of recommendations and conclusions are presented.

## 2 Protection of consumer data stored in cloud computing servers

In a cloud computing environment, consumers of the technology face many risks regarding the confidentiality, privacy, and susceptibility to data loss of their information. The consent to store one's data on the cloud entails placing the data under the control of a third party. The third party is implicitly trusted by the consumer, despite the consumer not knowing exactly where the data are stored. The cloud computing service provider will also have the right to transfer the data of the consumers from one location to another without notifying the data owner. Data could also be transferred to a governmental entity based on a judicial order (O'Meara, 2014). A judicial order can force the cloud computing service provider to release the private information of its customers.

In most cases, a consumer signs cloud computing contracts without objection and without full awareness of the terms of those contracts, complying to all the policies set by the service provider (Bradshaw et al., 2011). These contracts often contain arbitrary conditions that the consumers of the cloud computing services cannot negotiate or discuss, particularly with regard to the service provider's responsibility in the case of data loss or destruction. In the interest of transparency, there needs to be a reformulation of these contracts along with an examination of ways in which the consumer can be compelled to carefully read the terms of these contracts. In addition, the service provider often transfers the consumers' data to the servers of another subcontractor, which raises the question of the accountability of the service provider for privacy vulnerabilities created by the subcontractor. In addition, service providers reserve the right to change the terms of the service or the privacy policy without notification, and the consumer must accept these changes.

This raises the following two questions: what level of security and privacy is provided for the consumers, and what are the roles of legislation and policies implemented by service providers in providing data privacy and protection? The answer to these questions requires:

- analysis of cloud computing services under national laws and European directives and an examination of how useful these laws are in providing personal data protection and consumer privacy
- scrutinising privacy policies adopted by companies and websites
- exposing legal loopholes contained in legislative regulation and self-regulation, which may affect the level of privacy and protection provided for users and help cloud computing service providers avoid responsibility in cases of data loss or privacy invasion.

It is important to examine the level of responsibility that is incurred by cloud computing service provider in cases of data loss or privacy invasion. This will be followed with recommendations for amendments to some of the existing regulations in order to put more liability on cloud computing service providers.

The provision of data security and consumer privacy in cloud computing is a very important topic. Cloud computing, by its nature, is global and serves consumers and companies of all types across the world. The service provider can transfer consumer data from one location to another according to its own judgment, and as mentioned earlier, there are no strict rules established for the protection of personal data in a cloud computing. This raises an important question regarding the possibility of labelling data stored in the cloud as falling under the scope of laws covering personal data. It is important to consider whether the processes and regulations applied by European and national laws protecting personal data can be directly applied to data stored on cloud computing services. Finally, it is also important to question whether the correct regulation is in place to cover the transfer of data from one server to another.

At first glance, it may seem an obvious conclusion that data stored on a cloud computing service is personal data that deserves protection, however the nature of how cloud computing operates requires the subject to be further examined.

Personal data is a broad concept. In fact, the identity of a person can be recognised indirectly by the usage of cookies, which allows the collection of data that indicates the identity of the person. In addition, the identity of the person can be established directly at the time of signing the cloud computing service contract when the service provider collects the consumer's information directly by asking for details such as their name, job title, and address.

In addition, technological development has involved identity being further imprinted on information, contributing to the ability to identify a person. The availability of this data today is a problem that raises the question of whether to consider such data personal or private. Many websites using cloud computing technology such as Facebook are allowed to share this data under certain conditions (De Filippi and McCarthy, 2011). Data must be of a personal nature and must meet certain criteria to be considered for protection according to the rules governing this subject. The data is required to have been through a processing procedure that includes collection, storage and usage of the data by the service provider or its representative. Given this broad concept, there is no doubt that the provisioning of cloud computing services entails the necessity of processing personal data. Information is stored, recorded, or erased at the end of the contract.

In cloud computing, policies and technology are used to achieve the highest levels of digital security possible. This can be done through the adoption of the best standards and protection systems, so that data is protected from modification by unauthorised persons.

This can also be done by ensuring that the devices or servers used by the service provider are sufficiently secure and cannot be accessed without permission and ensuring that the data is of different consumers is not mixed. It should be the responsibility of the service provider to guarantee data integrity and security.

European directives and some national legislation have regulated the protection of personal data in general. Although this legislation has not been sufficient in some cases, it has already formed a legal framework that could be developed further. As previously mentioned, the non-existence of specific legislation for the full liability of the service provider in the cases of data loss and privacy violation is one of the central themes of this paper. However, many websites have adopted a self-regulatory approach developed from the policies they follow, and this is made visible to the consumer. These approaches will now be examined further.

Apart from external attack, the cloud environment is vulnerable to internal attack, too. For instance, cross VM attack is a major cause of data breach in cloud. Since cloud providers allow multi-tenancy, in which multiple clients are authorised to share same physical resources, information of each customer is vulnerable to other clients who share the same physical resources of the cloud provider (Xiao and Xiao, 2013). Lack of control is another privacy concern in cloud since the cloud user has little or no control over the stored data, which can be easily altered, modified or copied by the provider. Principals cloud security attacks were against its infrastructure, its transportation to or from cloud, and against user's data (Sub et al., 2019).

Table 1 lists few privacy challenges associated with cloud computing and their possible solutions (Zhou et al., 2015).

**Table 1** Privacy concerns and prevention techniques

| Privacy concern | Prevention technique |
|---|---|
| Identity protection | Group signature, anonymisation of the connection |
| Location privacy | Trapdoor permutation |
| Data integrity | Encryption |
| Layer removal or addition attack | Combined transmission evidence |

The two major challenges in implementing security to protect the privacy of users in cloud environment are efficiency and complexity. The use of the highly sophisticated privacy protection technique, such as encryption (Saleem et al., 2014), can slow down the overall system and reduce the efficiency and productivity (Alrabaee et al., 2014). Access to the control and encryption can reduce the speed of an access and increase the cost of cloud. On top of everything, implementing high-end data protection and privacy management scheme is utterly complex in cloud computing because of its vastness, scale, and ubiquity. It is not possible to implement full-proof plan to protect the privacy of user data without compromising many advantages of cloud. Thus, the main objective of this paper is to propose a deterrent approach that might deter attackers from committing a cyber crime before preventing by different prevention techniques mentioned earlier.

There are many privacy attacks that cost big companies, such as eBay, Adobe, Target and other companies millions of dollars ('World's Biggest Data Breaches', Information Is Beautiful, blog, 4 July 2018), and in the era of artificial intelligence, robotics, augmented reality (AR), big data and Internet of Things (IoT), cloud of things (Mohanasundaram et al., 2019), the risks of data leakage are much higher (Onik et al., 2019). During the

years between 2011 and 2015, a total of 227 data leakage occurred in the public sector, where around 80 of them are with unidentified number of records leaked, while for the other 147 data leakages an approximately of 6.9 million records were leaked (Joseph, 2018). And after Google vs. Vidal-Hall case in 2015, there would be a chance that a customer that is affected by the data leakage could receive a financial compensation for distress and humiliation caused by this leakage only and in some cases this could affect the company millions of dollars (Evans, 2015).

There are four different phases govern the emergency management which are the preparedness, mitigation, response, and recovery (Lindsay, 2013). These four phases cover the process of managing what should be done before, during and after the cyber attack. This is written in different laws and policies, but there is still a gap in these laws that should be fixed.

Privacy rights clearinghouse (PRC) is an organisation established in California that provides information regarding all the attacks and data breaches for all types of businesses (Privacyrights.org, 2020), including but not limited to educational, government, healthcare and other types of businesses. Table 2 is showing some data breaches that happened in the years 2017 and 2018, where attacks performed either unintentionally or by an outside party.

**Table 2** Some data breaches occurred in the last three years

| *Attack year* | *Company affected* | *Hack type* | *Type of organisation* | *Number of records compromised* |
|---|---|---|---|---|
| 2018 | Capital One | No info. was exposed | UNKNOWN | 500 |
| 2018 | JP Morgan Chase Bank, N.A. | No info. was exposed | UNKNOWN | 500 |
| 2018 | Bank of the West | No info. was exposed | UNKNOWN | 500 |
| 2018 | Reddit, Inc. | No info. was exposed | UNKNOWN | 500 |
| 2018 | Morgan Stanley smith barney LLC | No info. was exposed | UNKNOWN | 1 |
| 2018 | Los Angeles Philharmonic | No info. was exposed | UNKNOWN | 2,442 |
| 2018 | GHG Grey health group llc | No info. wase xposed | Medical | 683 |
| 2018 | Cedarville University | No info. was exposed | Educational | 241 |
| 2018 | Beach body LLC | Hacked by an outside party | Retail merchant | 854 |
| 2017 | Erie County Office of Children and Youth | Unintended disclosure | Government | 30 |
| 2017 | Verizon | Unintended disclosure | Other businesses | 6,000,000 |
| 2017 | Stanford University | Unintended disclosure | Educational | 10,000 |
| 2018 | FedEx | Unintended disclosure | Retail merchant | 119,000 |

## 2.1 At the level of European directives

Due to the importance of protecting consumers' personal data, cloud computing has received considerable legislative attention. The European directive provides a regulatory framework aimed at providing a high standard of protection for the privacy of individuals in member states and the free circulation of personal data within the framework of the European Union, ensuring the same level of protection across member states (Gerber, 2013).

The European strategy for cloud computing was proposed by the vice president of the European committee responsible for the digital agenda. The strategy proposed a comprehensive and practical plan for the development of cloud computing in Europe, the establishment of a European public-private partnership, and setting unified rules in Europe to establish a legal system that ensured data protection and privacy (Gerber, 2013). It also suggested that the mandate of the judiciary should also be applied, and the European union should play a greater role in unifying standards, encouraging the public sector to benefit from cloud computing (Celestine, 2013). The EU provides a high level of protection for personal data and imposes obligations on the service provider and companies to protect sensitive data stored via cloud computing (King and Raja, 2013).

European legislation offers two levels of protection. Obligations are imposed on companies that collect, use, exchange, or share data, and the legislation also provides more effective and robust protection for sensitive data. However, applying the 1995 European directive is costly and includes routine procedures that can impede business and may interfere with freedom of expression. In these respects, it is different to the USA model, which allows freer data flow in comparison. The methods used to process data and ensure its transparency are inefficient and old, and the definitions contained in it are non-specific and simple (Gerber, 2013). Setting limitations on the location of data storage is incompatible with the nature of cloud computing services and is expensive to implement. These limitations are not suitable for the nature of cloud computing as they restrict its spread and give a false impression of security and safety. Europe needs to be freed from these limitations (Celestine, 2013).

## 2.2 Emergence of GDPR

On 26 April 2016, the European parliament and the council of Europe adopted the GDPR [Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),which provided regulation on the protection of persons against the processing of personal data and the free flow of such data. The GDPR has been effective from 25 May 2018, and concerns data protection and privacy for all individuals within the European Union and the European Economic Area (Shastri et al., 2019). It replaces the Data Protection Directive of1995.It aims primarily at granting citizens and residents' control of their personal data and simplifying the regulatory environment for international business through the harmonisation of regulations within the EU. It includes the terms and conditions for the processing of personally identifiable information within the European Union.

This regulation gives internet users more rights, especially in terms of privacy in the midst of scandals of exploiting the personal data of consumers without their knowledge.

It will provide some of the most stringent internet privacy rules in the world and give consumers additional tools to control the information collected, with companies punished through the imposition of heavy fines of up to 4% of revenue.

The purpose of this regulation is to protect natural persons in the processing of their personal data, fundamental rights and freedoms, regardless of their nationality or place of residence, in particular their right to protect their personal data. It also aims to contribute to the achievement of freedom, security, and justice to create trust that allows for the support and development of the EU's digital economy, given the high risks to people's data. This regulation is designed to ensure an appropriate level of protection and removal of obstacles to personal data flows within the European Union and to ensure the harmonious and consistent application of laws relating to the protection of the fundamental rights and freedoms of natural persons in relation to the processing of personal data in all EU countries.

### *2.2.1 The scope of GDPR*

The GDPR covers all companies dealing with data from EU citizens for transactions occurring within EU member states, especially banks, insurance companies, and other financial companies. Beyond this, it has become a major influence on all visitors to internet sites without exception, regardless of where the business is established.

The regulation applies to any personal data such as name, social security number, site data, online identifier (IP address or e-mail address), or one or more special factors of the physical, physiological, genetic, mental, economic, cultural, or social identity of the person. The regulation aims to give the consumer full control over their own data. Companies will not be able to obtain any data from the consumer without prior consent (Article 4). The regulation applies to sensitive personal data such as nationality, ethnic origin, sexual orientation, and health status (Article 9). The regulation does not apply to the processing of personal data from a natural person during a purely domestic or personal activity, which may include correspondence, access to addresses, social media, and online activity within the context of such activities. It also does not apply to control units or processors that provide the means to process personal data for such personal or household activities.

The principles of the regulation protect data on an identifiable person. Natural persons may connect with identifiers on the internet related to their own devices, applications, tools, and protocols, such as IP addresses, file identifiers, or other identifiers such as wireless frequency identification cards. This may leave traces of evidence, especially when associated with unique identifiers or other server information, which can be used to create profiles or identify natural persons. The data owner's express consent must therefore be given to deal with their personal data, such as a written statement, including electronic means or an oral statement. This may include marking when one visits a website, selecting technical settings on an information service, or other statement or behaviour that clearly shows the acceptance of the proposed treatment of the personal data of persons whose data are registered. Inaction or non-activation shall not constitute any consent. Approval can occur for processing multiple activities carried out for the same purpose, but for processing activities for several purposes, approval must be granted for each.

### 2.2.2 Rights of consumers under GDPR

Regulations cover the right of the data holder for any processing of personal data to be lawful and fair (Duncan, 2018). They must be transparent to natural persons. The principle of transparency requires that any information relating to the processing of such personal data be easily accessible and understood and in simple and clear language. In particular, this principle concerns personal data that can be used for identification of the user, the processes and purposes of treatment, and access to further information to ensure transparent and fair treatment of the natural persons concerned. Their right to obtain assurance and communication about their personal data must also be assured. Natural persons must be aware of the risks, rules, guarantees, and rights relating to the processing of their personal data and the manner in which such rights are exercised. In particular, the specific purposes for processing personal data must be explicit, legitimate, and specific at the time of collection of the personal data, and personal data must be sufficient, relevant and limited to what is necessary for the purposes addressed. This requires, in particular, that the period in which the personal data is stored is strictly limited. Personal data must only be processed if the purpose of the treatment cannot be reasonably accomplished by other means. Personal data must also not be saved too long.

Personal data must be processed in such a way as to ensure proper security and confidentiality, including the prevention of unauthorised access to, or the use of, personal data or equipment used in processing. In any case, the methods of processing must be legal, based on the consent of the person who owns the data, and in accordance with other legal circumstances. The new law requires companies to be transparent about how to deal with consumer data and obtain their permission before starting to use it. The new law also gives the consumer the right to know which of their personal information they hold, and to delete it if the owner so desires. These procedures apply not only to technology companies, but also to banks, retailers, and any other organisation that stores consumers' information.

- *Approval and acceptance:* There must be explicit consent from the consumer prior to data collection and prior to data use. These must be explained to the consumer in a language they understand without any deception or words that carry more than one meaning, and a cogent reason for processing or storing personal information must be provided.
- *Right to be forgotten:* Consumers are allowed to request that their personal information be fully deleted. This is also referred to as the right to be forgotten as in Article 17 (Duncan, 2018). Companies are required to execute the request and delete the data. If this data is used by other parties, companies must send the request to them to delete the consumer's content and data based on their desire.
- *Right to know:* Consumers have the right to know what information is stored on them, which is done with explicit permission from them to do so.
- *Privacy by design and default setting (Al-Sharieh et al., 2018):* New systems must have protection based primarily on strict data access control and access must only be granted when needed. Business processes that deal with personal data must be created with privacy standards by design. By default, personal data must be stored using an alias or full identity, and the highest privacy settings enabled by default, so that the data is not publicly available without explicit consent and cannot be used to

derive personal information without storing additional information separately. No personal data may be processed unless it is done on a legal basis determined by the regulation, or if the data controller or processor receives explicit approval from the data owner. In case of data loss, theft, or unauthorised access, the authorities must be notified within 72 hours (under Article 33) together with the persons whose data has been accessed (Article 34). Data can be used only for the reasons provided at the time of collection and deleted securely when no longer needed.

- *Access to and transfer of data:* Any person may request his or her personal data in a format that can be easily downloaded at any time and can also be used with or transmitted to any other site or service (Article 20). National authorities are allowed to impose fines on companies violating the regulation. Parental consent will also be required to process personal data of children under the age of 16 for online services; this may vary according to the member's status, but not below 13 years (Article 8).
- *Companies are subject to EU law if:*
  1 the company's business has presence in the EU
  2 if the company is dealing with the personal data of the European population, even if there is no physical presence in the EU
  3 the company has more than 250 employees
  4 if the processing of company data affects the rights and freedoms of the persons concerned even if the number of employees is less than 250.

The new data protection law requires social media companies to have a representative before the EU who can be held accountable for their company's compliance with GDPR laws within Europe. The most obvious changes in terms of use give the consumer new authority to approve any data usage, which means that companies will not act on any data except with their express permission, and in a way that is completely transparent. The consumer will also be able to download all the data owned by the company and help to verify the companies that collect data as well as the removal of the boundaries between companies and the ability to share data between services. The most important changes will be out of sight of the public. The law states how companies can share consumer data after collection, which means that companies will rethink how to handle data, sign-ins, and ads. This could lead to a gap between the EU and other internet consumers in that they will see a different version of the internet from the rest of the world; many consumers within this range can already see a change in usage policy.

The General Regulations for the Protection of Personal Data will provide significant control features parallel to what companies do with their data. They combine a number of different concepts, including the right to correct data, the ability to make decisions that include the right of customers to maintain or abstain from records, and what will be done with the data listed. These regulations will have a significant impact on companies in terms of customers and partnerships. It would therefore be better for companies to ensure their compliance with the general data protection regulations, and to ensure that other organisations and companies achieve full compliance with the regulations themselves to join their partners with a view to securing official recognition, as well as to enjoy all features and services under these terms (Duncan, 2019). Compliance with the general data protection regulations should not be seen as an impediment, but rather as an opportunity, providing organisations with a great opportunity to update their systems and

make use of data, which in turn will result in a new approach that will significantly change companies and improve their security.

The law applies to any company established within the European Union, any organisation that sells goods or provides services to people within the European Union, and anyone who monitors the behaviour of anyone within the European Union. An example is Microsoft, a leader in cloud computing, which provides customer systems and processes customer data on behalf of its customers as well as governments. Solutions include Dynamix 365, Office 365, and the Microsoft Azure cloud platform. All companies that have a presence on the internet, including large US companies such as Microsoft, Google, and Facebook, must comply with the new law. Many large social media and other online companies have updated their privacy policies and terms of service. Companies such as Facebook, Microsoft, Twitter, Apple, and others outside the EU have provided some additional consumer rights regarding data, but these rights are not monitored by a strict law such as GDPR, which means that one cannot file a complaint if one is not a resident of the European Union. However, what is certain is that companies will need to work more to demonstrate that consumers have understood and agreed to their terms of use.

The right to data transfer allows individuals to access their personal data and reuse it across different services. The right to be forgotten or the so-called 'right to erase' means individuals can now request that their personal data be erased or not used in certain circumstances. Although there are several exceptions to this, it is based in the right of forgetfulness, which was established in the jurisprudence of the European Court of Justice in 2014.

In the event of a breach of personal data that is likely to have adverse effects on the individual (such as damage to reputation, loss of confidentiality, or financial loss), the organisation will need to report this breach to affected individuals, as well as the relevant supervisory authority, or face a fine.

Direct Representation by NGOs: Consumers throughout the EU are now entitled to request for competent non-governmental organisations to file claims against data processors on their behalf. States can also grant these NGOs the right to bring collective cases. This will lead to a significant increase in the number of lawsuits immediately after this provision becomes effective.

The European economic and social committee has given a written opinion on cloud computing in Europe as a future vision in 2020. There are several weaknesses in cloud computing, with a lot of standards for regulating them that lack a specific unified authority to govern and control the environment. Another weakness is the lack of information for cloud computing users that shows them the risks of using them and the risks of transferring their own data to a third party. Information regarding rights and obligations with respect to the two parties involved in the cloud computing service contract is not clearly defined. However, the committee does highlight some advantages of cloud computing services, such as the provisioning and increase of the number of servers in Europe and the creation of a public partnership to promote EU research centres (Gerber, 2013).

### *2.3 At the level of USA legislation*

The US legislature has enacted several laws to regulate the protection of personal data. The Privacy Act of 1974, (18 USC 2510-2522) and the Privacy Act of 1986 (50 USC

1862)., state that it is prohibited to disclose any information handled by the information system by any means to any person or to any other entity unless written consent by the data owner exists, it is in the public interest, or it has been ordered by the courts.

US law has determined a set of guarantees to protect data, such as requirement for written consent for data transfer and the obligation of government agencies to notify the data owner of the purpose of the collection and their rights, such as the right of access and right of correction. The Patriot Act (Doyle, 2002) regulates the exchange of personal information and decides some exceptions that allow government authorities to view such data if certain justifications are available to do so, such as the public interest (Weiss and Archick, 2016). The US legislators also recognise the principles of Safe Harbor (Weiss and Archick, 2016), issued by the US Department of Commerce, in which national companies respect the European directive (De Filippi and McCarthy, 2011). There are some exceptions to give the US government the right to access the data stored on its territory in a state of emergency, or if it is deemed necessary to ensure national security under the Patriot Act (Segall, 2012).

During the Obama administration, the US government concentrated particularly on the privacy of internet users, issuing a 'bill of rights' for consumer protection in the FTC Report in 2012, and formed a proposal to regulate digital privacy globally. There is a need for mandatory restrictions, controlled by an organisation, on how privacy is effectively protected in cloud computing, and they must apply to the provision of cloud computing services between national borders (King and Raja, 2013), as laws do not restrict the transfer of data abroad. Companies in the US are free to transmit data to providers who may in turn transmit it to servers located in different countries. However, there is a possibility to apply the principles of Safe Harbor with regards to companies regulated by this agreement, which can provide an appropriate level of protection (McKenna, 2016).

The law governing the use of cloud computing and data storage in the USA is the Electronic Communications Privacy Act (ECPA) of 1986 (Calloway, 2012). The privacy act was amended in 1996 to provide better protection and stronger standards and was further amended by the 2001 Citizenship Act and the Reauthorization Act of 2006 and the 2008 Amendment. The ECPA prohibits the disclosure of any electronic communications, imposes certain procedures for obtaining an authorisation to disclose any electronic communications, and imposes various penalties for violations.

However, the definition of a violation is broad and depends on an old understanding of the nature of communication, with courts having faced problems applying the law (Morgan, 2016). The basic problem in the law is that it depends on an old understanding of the word 'communications'. The law is old and has been rendered obsolete by the rapid development of modern technology (Celestine, 2013).

Part II of this legislation covers the Stored Communication Act (SCA), which protects communications held in electronic storage. This law protects the privacy of file content stored through service providers, prohibiting them from disclosing communications without permission or approval (Gerber, 2013). The interpretation of this law is difficult and contradictory, because its application with regards to cloud computing depends on the definitions of remote cloud computing and electronic communication services, which are out of date.

Also, of note is the Computer Fraud Act, which criminalises intentional computer-based espionage against the US government, unauthorised access to computer systems and government agencies, access to a protected computer to destroy or acquire

valuable information, and transmission of a virus. The CFAA Act determines criminal penalties for individuals or entities that breach computers for the purpose of damaging them or with the intent of performing unauthorised data access, but this law must reflect modern methods of computer related crimes. The act is outdated and imposes the same penalties against those who penetrate individual data and the data of a data centre (Segall, 2012).

The Code of Personal Data, Violation of Legal Matters 2011, the Notice Breach Act, the Data Notification Act 2011, the HIPAA Data Privacy Rules, and the GLBA Act are also referred to as placing multiple restrictions on cloud computing contracts. The US government has adopted a special plan covering cloud computing called 'cloud computing first' (Rutter, 2012).

It has been noted that US privacy and technology laws are sectoral laws (Weiss and Archick, 2016) and are regulated by various clusters of laws or by self-regulation. Citizenship law affects the cloud computing industry. The US government has tried to self-regulate its own use of cloud computing, in accordance with the 'cloud computing first' plan. It is challenging to create universal regulation with legislative balance covering cloud computing.

There is a difference between US laws based on freedom of expression and European laws that focus on the protection of personal data and prevent or restrict transferring data abroad. European laws are inconsistent with US laws, which may result in contradictions between the two if an institution has a presence in both regions (Rutter, 2012). In Europe everyone has the right to a private life, and legislation in each country restricts the process of processing data on a specific person. Any information belonging to a specific person is protected within the European Union, but in US law, the issue relates to the right to expression in the first amendment. Only certain types of data are protected, such as health data, children's data, and financial data (Rutter, 2012) and there are many exceptions to this right, such as the purposes of investigations, statistics, records and the Patriot Act. An employee's e-mail can be read by the employer if it is sent during work hours from a work computer, especially if the worker has been warned. This type of practice is totally unacceptable in Europe (Celestine, 2013), as indicated by an appeals court in France (Chevalier, 2016).

The European perspective is a constraint on business, whereas the US perspective does not prioritise consumer protection, and ultimately it must be noted that the protection varies from one legal system to the other. The resulting legislative acts at the national and international level have not been sufficient to ensure effective protection of personal data. In the US, technology is generally allowed to evolve, with some rules to address these concerns. As for the reasons for the differences in the legal organisation of privacy in Europe, they may be psychological, political, and influenced by pressure groups and lobbies.

It should be noted that the process of transferring data abroad increases the risk to the consumer's data. Data transferred to a server outside the European Union may be held in a country with an appropriate level of protection such as Canada, Switzerland, or Argentina. In France, prior authorisation is also required from the CNIL (Sordet and Milchior, 2012). To transfer data to the USA, the service provider must apply the principles of Safe Harbor or obtain authorisation from the data owner to transfer the data abroad. It is in the consumer's interest to ask the service provider to store the data on servers within the EU, and for the data not to be given to anyone.

The beneficiary of cloud computing should ensure that there is a term in the cloud computing contract to ensure privacy and the determination of a subcontractor if needed (King and Raja, 2013). The end of a cloud computing contract raises concerns that the data will remain with the provider. Therefore, the contract must include a term to return or destroy the data once the contract expires.

One of the loopholes that is emerging in the context of legislative regulation of the protection of personal data in cloud computing is the existence of regional law issues in Europe and the US that restrict companies from providing transnational computing services in the context of the growing development of this industry (Bradshaw et al., 2011). The location of the data may go beyond national boundaries. In addition, in transmitting the data abroad, the data may be exposed to safety breaches. This paper will now go on to examine the use of self-regulation to protect privacy in cloud computing.

## 3 Research gaps

The research gaps at both international and national levels are summarised in the table below and the recommendations are also specified to enhance these laws as shown in Table 3 and Table 4.

**Table 3** Most important conventions and directives at the international level

| | *Issue year* | *Objective* | *Gaps* | *Recommendations/scope* | |
|---|---|---|---|---|---|
| OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data | 1982 | Protection of privacy and private data. | Recommendation non-obligatory to countries members. | *Scope* | The public and private sectors. The principle was limited to personal data which because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties. |
| Data protection Directive No. 46/95 | 1995 | Personal data protection.<br>• Transmission of Data of European citizens aboard. | Complexity, inefficiently, indeterminate<br>Divergence between member states in application, costly. | Increasing the effectiveness of the data protection in the context of technological developments.<br>*Scope* | All processing of personal data wholly or partially by automatic means and to the processing by other means of personal data in or intended for a filing system – carried out in the context of the activities of an establishment of the controller on the territory of an EU Member State |

**Table 3** Most important conventions and directives at the international level (continued)

| | *Issue year* | *Objective* | *Gaps* | *Recommendations/scope* |
|---|---|---|---|---|
| General data protection regulation | 27 May 2016 | Protect 'natural persons' with regard to processing of personal data and on free movement of such data.<br>Data minimisation<br>Right to be forgotten<br>Privacy by design<br>Clarification of 'consent' | European citizens | Enforced on 25 May 2018.<br>All processing of personal data wholly or partly by automated means, and to the processing by other means of personal data in or intended for a filing system, private and public sector. |

**Table 4** Important laws and acts at the national level

| *Country* | *Name of law/act* | *Issue year* | *Objective and scope* | *Gaps* | *Recommendations-update* |
|---|---|---|---|---|---|
| France | Act No 78-17 on Information Technology, Data Files and Civil Liberties | 6 January 1978 | The processing, automated or not, of personal data contained or intended to be part of a personal data filing system. From the private and public sectors carried out by a natural person or legal entity, where the data controller is established on French territory. | Non-determined conceptions | Amended by Law 2004-801 of August 6, 2004, and amended by Law No 2016-1321 for a Digital Republic dated 7 October 2016. |
| | The Privacy Act. | 1974 | Organisation of collect, use of personal data in USA. | Sectorial laws.<br>Industry-specific protection.<br>Narrow scope. | To the records of every 'individual', held by an 'agency' |
| | The Electronic Communications Privacy Act of 1986 (ECPA) | 1986 | Protection of private data over electronic communication systems. | Difficult Interpretation and contradictory | |

**Table 4** Important laws and acts at the national level (continued)

| *Country* | *Name of law/act* | *Issue year* | *Objective and scope* | *Gaps* | *Recommendations-update* |
|---|---|---|---|---|---|
| USA | The Patriot Act | 26 October 2001 | Antiterrorism law, to help government agencies detect and prevent possible acts of terrorism, or sponsorship of terrorist groups | Affecting freedom and damaging data can expose it to the public interest. | |

## 4 Self-regulation of personal data protection and the role of companies providing cloud services

The purpose of the study is to examine the evolution of privacy policies and terms of use issued by service providers in order to clarify whether they provide better or less privacy protection. A range of terms of use, which are frequently employed by cloud computing service providers, will be discussed to illustrate their drawbacks.

### *4.1 The development of privacy policies, corporate initiatives, and websites*

Self-regulation and privacy policies adopted by companies play an important and complementary role in protecting personal data. In the USA, the role of companies and the importance of their policies in protecting data, especially in the private sector, are increasing, although they are not sufficient to provide adequate protection for cloud computing users. In many cases the consumer does not read or understand what is written and is not interested in the content of cloud computing contracts (Rohrmann et al., 2015). The majority of cloud computing contract terms tend to be for the benefit of the service provider. The providers reserve the right to change the standards without notifying the consumer, meaning that the consumer must compare the previous terms with the updated ones to know the difference. However, privacy policies can be important for websites and consumers, as they often provide the only protection to the consumer in the case of the absence of special legislation. Privacy policies consist of one or more documents and include the conditions governing the relationship between the consumer and the provider, including conditions of service, quality and continuity, privacy rules, rules on intellectual property, data integrity and confidentiality, and the responsibility to return and erase data at the end of the contract (Piper, 2015). The policies of cloud service providers are very similar, though differ in some details. Facebook, Yahoo, Google, Twitter, and Snapchat have their own privacy policies.

The website could also be part of what is called a consortium, which can be defined as a set of websites adhering to a single central privacy policy. In 2009, the European Information and Networks Security Agency identified several issues that a cloud computing contract should include, such as data protection, availability, safety, security, confidentiality, and protection of intellectual property (Bradshaw et al., 2011). It is worth mentioning that some contracts are not called cloud computing contracts but terms of use.

Some contracts refer to the privacy policy and responsibilities of the parties, and sometimes they may be independent documents as part of the cloud computing contract.

Service providers are sometimes required to sign contracts with sub-contractors. These contracts are confidentiality agreements that allow only authorised persons to access sensitive consumer data while performing their duties and exchanging documents between the parties, and the service provider has the right to monitor the subcontractors for any violations committed (Bradshaw et al., 2011). Privacy policies describe the service provider's measures on the use and collection of personal data, how they are protected, and how loss, damage, or deletion of the data is avoided. One of the companies that commits to providing the best service possible to ensure the integrity and confidentiality of data is Amazon, which places the whole responsibility on itself. In contrast, Microsoft places the responsibility on the consumer.

The issue of consumer data deletion at the end of a contract is a highly important subject for data owners. Everything about this issue should be clearly defined, such as the retention period of data, the requirement for removal, and assurances that it will not be stored on the service provider's servers. The policies adopted by companies show that some companies decide that the consumer will have access to the data or can recover it at any time, while other companies retain the data for a certain period of time after the end of the contract. Amazon retains the data for a certain period before deletion (Bradshaw et al., 2011), whereas other companies such as Apple delete the data as soon as the contract ends.

Some other companies do not commit to keeping the consumer's data after the end of the contract but also do not undertake deleting it, such as Microsoft and Google. Facebook saves the data of consumers who have died and allows for the limited publishing of comments on their Facebook profiles (Stylianou, 2010). With regard to the disclosure of stored data, most companies allow this on the basis of a court order or if a legal investigation needs some information on the consumer from a specific company. Sometimes it is necessary to notify the consumer of this, such as in the case of Twitter. As for the possibility of transferring data outside the country, it is noted that Amazon designates secured areas and guarantees data protection during transfer, and extends its commitment to Safe Harbor procedures, as is the case with Microsoft (Stylianou, 2010). Some service providers warn that data may be transmitted unencrypted in certain circumstances. Dropbox determines that all data transferred is encrypted and that the company takes concerns about safety seriously, not allowing anyone to access the consumer's files unless they agree to share the data.

When discussing policies to protect privacy and personal data, it must be noted that the majority of websites create obligations that are included in the privacy policies. These policies do not exempt websites from their legal liabilities and aim to inform the consumer that there is a legal framework for such protection. In most cases, the party that is responsible for the website refers to the legislation that the website adheres to. These policies are mostly a reaffirmation of national and international legislation governing the protection of personal data.

Privacy policies must be clear, comprehensive, and accessible through the website. The policies should focus on the website's commitment to the protection of personal data and privacy, the information collected, the restrictions on usage of the information, and the extent to which such information may be transmitted to others. The policy may also cover the extent to which cookies are used, the purpose of their use, the consumer's right

to object, withdraw information, and access data, the integrity of the website, and specific information about the legislation that the website adheres to.

Companies tend to make extensive efforts to provide high standards of professionalism to ensure privacy. When drafting contractual privacy conditions, however, companies argue that they must strike a balance between protecting privacy and monetising the available data. This is true of companies such as IBM, Microsoft, Amazon, Google, and Apple. Older privacy policies were governed either by the general terms of the company or by the general terms contained within a subsequent agreement for special services. Cloud computing service providers explicitly declare to the consumer that they use cookies but do not specify the nature or number of those cookies. IBM provides additional information about the possible collection of information through, or exchange of data with, a third party.

Some of the uses of the collected data are clear, and others are less well defined. In 2007, Apple added to its privacy policy that it could use information for analysis for the development of Apple products. Google's Gmail has been criticized, causing Google to change the words used in its privacy policies, stating that it only uses ads that employ its own technology. Previously, in 2004, Google stated 'Gmail and its services include ads and links based on IP, content of messages and other information associated with your use of Gmail'. In 2009, the company displayed how the data is handled regarding privacy in an attempt to reassure consumers. Google stated that it scans Gmail messages to filter spam, detect viruses, and filter keywords in consumer e-mail messages that are then used to link them to ads. There is no human intervention in this process (King and Raja, 2013). Amazon has added in its recent policies that cookies and related information can be used for personalised advertisements. Microsoft collects data by placing cookies on a consumer's computer and connects them with a consumer's visits, purchases, and activity. When running ads, it takes several steps to protect privacy, such as keeping views confidential, in the same manner as IBM.

Most companies have decided that it is important for the consumer to be able to have full control over their data, including the ability to remove their data from the website at their request. However, there is no uniform time limit for companies to complete this request. Some companies perform the deletion within 30 days of the request, whereas Gmail does not declare or set a time for deletion and admits that copies of e-mails could remain in the company's system even after the consumer has deleted them from the mailbox or after the account has been terminated. Google has since amended the Gmail privacy policy to state that deleted messages and accounts could take 60 days to be deleted from the company's active servers, and that they may remain within the offline retrieval systems. This provision has subsequently been removed in recent amendments to the policies.

As for data storage, companies require consumers to agree to transfer data to and from the USA and to respect secure transit requirements. However, it is not clear what level of protection is provided for consumer data when they travel around the world. IBM has determined that even in countries that set a lower level of protection, the company maintains consumer data in the way described above, but it is not clear how this is ensured.

For data security and integrity, the company may use cryptographic technology when transferring and storing data, the use of which IBM detailed in its latest policies. Amazon refuses to guarantee that content is secured for many reasons, so the customer is responsible for ensuring the integrity and retrieval of the data. Apple has decided that it

has the right to determine whether content is compatible with the terms of use and may refuse, modify, or delete content at any time without prior notification if the content violates the terms of use, or is offensive or has been contested.

Personal data protection policies can also be represented by the codes of conduct that a website adopts, which are often composed by the consumers themselves. These codes of conduct can be adopted by trade unions and professional institutions and by representatives of those responsible for data processing. These codes are subject to supervision by a competent authority. The majority of companies in the US are regulated by a select group of authorities, which is mandatory and subject to supervision by the Federal Trade Commission. As for certificates and documentation, some companies may use the so-called Trusted Third Party, which is a neutral entity that gives certificates, such as the so-called Truste and ISO 9001/ISO 9002 certificates, to a particular website, indicating the website's privacy standards. It has a logo, code, or seal for the benefit of consumers and ensures that the website is under the monitoring and supervision of third parties in respect to the protection of personal data and the integrity of transactions on their website. This logo is obtained voluntarily and there is no need for the website to obtain a certificate from others regarding the protection of personal data. The website that wishes to obtain the certificate is subject to a number of rules, including specifying its obligations regarding the protection of personal data, either by adopting a pre-existing policy or by adopting the model established by the certifying entity. It should also take into account many of the points highlighted by national legislation, such as Law no. 2004–575, of 21 June 2004, on the confidence in the digital economy ('LCEN law'). Programs that ensure anonymity are a set of technologies that allow the protection of data by means of a password. Information and data transmitted by a public or private key are evaluated and encrypted, which prevents unauthorised persons from accessing it.

### *4.2 Legal Gapsin self-regulation*

The following section will examine whether privacy policies in cloud computing services and self-regulatory methods are adequate and appropriate solutions for effective protection. Usually, agreements between service providers and consumers are used to reduce the risk of cloud computing with regards to privacy and data integrity while protecting sensitive data, but in practice consumers do not have the ability to negotiate terms of use with major providers such as Amazon, Microsoft, and Google, where there is a significant difference in negotiating or bargaining capabilities between the parties. It is common for service providers to focus on non-negotiable agreements, and the typical terms of use increase privacy concerns because they are pre-set by service providers. These terms cover the expected level of service provided by the service provider and the compensation facilities available to the customer in the case of a failure to provide a certain level of services, and the customer's ability to recover data or to ensure that it is deleted if the contract is terminated (Piper, 2015).

Therefore, there are obstacles in relying solely on the privacy policies and technologies available for ensuring the privacy and integrity of data in cloud computing. It is not practical for consumers of cloud computing services to negotiate with the service provider because of their comparatively weak negotiating stance (Piper, 2015). Self-regulation and cross-regulation provide economic advantages to the website, confer a degree of confidence to the consumer, and provide flexibility. However, these

regulatory methods remain an inadequate method of providing protection because of the absence of such principles in a wide range of websites.

Even when the stated privacy policy on a website contains obligations reflecting these principles, the policies themselves have exceptions that limit the effectiveness and obligations regarding the principles of protection. Further, websites engage in practices that discourage the reading of these policies, so this approach is complementary so as to fill the gap that exists in the practical application of the law.

## 5 Obligations of cloud computing service providers and liability in case of personal data privacy invasion

Personal data is often subject to inappropriate treatment by the data recipient or by a third party. This can occur through the process of collecting and storing data illegally, misuse, sharing and dissemination, and illegal trafficking. The recipient of personal data can use the data illegally by selling it or disclosing it to another person. The question here regards the extent of protection to be determined by the general rules provided for the data owner, the responsibility of each party who has been hacked, and the responsibility of the recipient of the data if there are conditions for liability exemption.

It should be noted that there are abundant theories that argue for the accountability of a personal data recipient that fails to protect the data, where it is possible to determine the level of responsibility for compromising personal data according to the general rules mentioned in civil code, or based on special rules that address the responsibility of internet service providers, as mentioned in the European directive for e-commerce in 2000. These laws impose a special system of responsibility for service providers that depends on the distinction between what could be considered as a positive or negative role of the provider.

It is necessary to stipulate special conditions to specify who is accountable for a fault based on actual knowledge of illegal content and the failure to act quickly to delete or withdraw the content. In these circumstances cloud computing service providers can be considered as providers of hosting services (Piper, 2015), a negative role, which ensures they are not responsible for the content of electronic data storage, with the service provider being fully responsible only if it is proven that they are aware of the illegality of the content and did not block access or remove it in response. The data recipient's responsibility towards the data owner must be contractual and all the terms of the contract must be taken into account according to the principle that the contract is the legislation of the contractors.

## 6 Conclusions and recommendations

Many legal issues have been discussed in this paper to illustrate the disadvantages existing in the current laws for private companies, both at a national legislative level and at the international legislative level. The paper makes the recommendations below and highlights the disadvantages of each of the aspects discussed in the previous sections. This paper can be used as a reference by any service provider in the private or public sector to improve their standards, to reassure the consumer of a cloud computing service in which their data is securely held.

1 There is a necessity for the existence of a global organisation that applies cloud computing principles on a global basis and reduces the impact of national laws that may limit trans-border transactions.

2 Adopt comprehensive legal regulation to protect personal data in the USA and improve the application of the citizenship law through cloud computing.

3 Review the EU's restrictions on data transfer abroad to remove unnecessary restrictions on the spread of cloud computing.

4 Simplify, clarify, and standardise the US Privacy Act and provide sturdier communication and data protection to create appropriate standards for privacy and data integrity within cloud computing.

5 Give consumers the option of choosing data storage location.

6 Contract law and liability may play an important role in determining the legal framework applied in cloud computing and service provider liability.

7 Direct government intervention must be reduced in dictating the privacy policies of cloud computing as much as possible, because it stops the development of cloud computing and reduces its flexibility. The private sector should be allowed to participate in the development of codes of conduct and standards of practices. This is could be accomplished in case of failure to establish a global organisation that governs the assurance of consumer data privacy.

8 Review sanctions and the concept of violations to be more compatible with modern technological developments.

## References

(2018) 'World's biggest data breaches', *Information Is Beautiful*, blog, 4 July [online] http://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks (accessed 11 May 2020).

Alrabaee, S., Khateeb, K. and Khasawneh, F.A. (2014) 'Preserving database privacy in cloud computing', in Editor, A. (Ed.): *Proceedings of International Conference on Security in Computer Networks and Distributed Systems*, Berlin, Heidelberg: Springer, pp.485–495.

Al-Sharieh, S. et al. (2018) 'Securiting the person and protecting the data: the requirement and implementation of privacy by design in law enforcement ICT system', in Mifsud Bonnici, J., Cannataci, J. and Wieh-Graz, N.W.V. (Eds.): *Chapter 8, Changing Communities, Changing Policing*, p.174.

Anomelechi, N. et al. (2018) 'A management view of security and cloud computing', *Proceedings of the Ninth International Conference of Cloud Computing, GRIDs and Virtualization*, p.27.

Bradshaw, S., Millard, C. and Walden, I. (2011) 'Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services', *International Journal of Law and Information Technology*, Vol. 19, No. 3, pp.187–223.

Calloway, T. (2012) 'Cloud computing, clickwrap agreements, and limitation on liability clauses: a perfect storm', *Duke L. & Tech. Rev.*, Vol. 11, No. 1, p.163.

Celestine, C. (2013) 'Cloudy skies, bright futures: in defense of a private regulatory scheme for policing cloud computing', *U. Ill. JL. Tech. & Pol'y*, Vol. 2013, No. 1, p.141.

Chevalier, M. (2016) *Les enjeux juridiques concernant les nouveaux modèles d'affaires basés sur la commercialisation des données*, 2015, Mémoire Université de Montréal, Montreal, Canada.

De Filippi, P. and McCarthy, S. (2011) 'Cloud computing: legal issues in centralized architectures', *VII International Conference on Internet, Law and Politics*.

Dorairaj, S.D. and Kaliannan, T. (2015) 'An adaptive multilevel security framework for the data stored in cloud environment', *The Scientific World Journal*, Vol. 15, pp.1–11, Article ID 601017.

Doyle, C. (2002) *The PATRIOT Act: A Legal Analysis*, Congressional Research Service, Washington DC.

Duncan, B. (2018) *Can EU General Data Protection Regulation Compliance be achieved When Using Cloud Computing*, p.2, Cloud Computing Conference, At Barcelona, Spain.

Duncan, B. (2019) 'EU general data protection regulation compliance challenges for cloud users', *Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, pp.27–28.

Evans, K. (2015) 'Vidal-hall and risk management for privacy breaches', in *IEEE Security & Privacy*, September–October, Vol. 13, No. 5, pp.80–84.

Gerber, J. (2013) 'Head out of the clouds: what the United States may learn from the European Union's treatment of data in the cloud', *Ind. Int'l & Comp. L. Rev.*, Vol. 23, No. 2, p.245.

Joseph, R.C. (2018) 'Data breaches: public sector perspectives', in *IT Professional*, July/August, Vol. 20, No. 4, pp.57–64.

Kanimozhi, R. (2019) 'Adaptive and intelligent framework of data protection techniques for cloud storage', *International Journal of Cloud Computing*, Vol. 8, No. 1, pp.50–67.

King, N. and Raja, V. (2013) 'What do they really know about me in the cloud? A comparative law perspective on protecting privacy and security of sensitive consumer data', *American Business Law Journal*, Vol. 50, No. 2, pp.413–482.

Law no. 2004-575, 21 June 2004, on the confidence in the digital economy ('LCEN law') https://wilmap.law.stanford.edu/entries/law-no-2004-575-confidence-digital-economy-loi-pourla-confiance-dans-leconomie-numerique.

Li, J. et al. (2017) 'Towards privacy-preserving storage and retrieval in multiple clouds', *IEEE Transactions on Cloud Computing*, Vol. 5, No. 3, pp.499–509.

Lindsay, B.R. (2013) *Federal Emergency Management: A Brief Introduction*, USA.

McKenna, M. (2016) 'Up in the cloud: finding common ground in providing for law enforcement access to data held by cloud computing service providers', *V and. J. Transnat'l L.*, Vol. 49, No. 5, p.1417.

Mohanasundaram, R. et al. (2019) 'A survey: comparative study of internet of things and cloud of things', *International Journal of Cloud Computing*, Vol. 8, No. 3, pp.237–248.

Morgan, W. (2016) 'Baring all: legal ethics and confidentiality of electronically stored information in the cloud', *Catholic University Journal of Law and Technology*, Vol. 24, No. 2, p.8.

O'Meara, G.J. (2014) 'Some silver linings have clouds: common law confidentiality in a fiduciary frame, attorneys, and cloud computing', *Creighton L. Rev.*, Vol. 48, No. 4, p.793.

Onik. M.H., Kim, C. and Yang, J. (2019) 'Personal data privacy challenges of the fourth industrial revolution', *Proceedings of 21st International Conference on Advanced Communication Technology (ICACT)*, Pyeong Chang Kwangwoon_Do, Korea (South), pp.635–638.

Piper, D.L.A. (2015) *Comparative Study on Cloud Computing Contracts*, March, Final report, European Commission, UK.

Privacyrights.org (2020) *Data Breaches, Privacy Rights Clearinghouse* [online] https://privacyrights.org/data-breaches (accessed 15 February 2020).

Rohrmann, C., Cunha, S. and Falci, J. (2015) 'Some legal aspects of cloud computing contracts', *J. Int't. Com. L. & Tech.*, Vol. 10, No. 1, p.37.

Rutter, B. (2012) *The Contrasting Environments for Cloud Computing in the United States and Europe: Jurisdiction and Contrasts*, Doctoral thesis, McGill University, Montreal.

Saleem, N., Alrabaee, S., Khasawneh, F.A. and Khasawneh, M. (2014) 'Aggregation function using Homomorphic encryption in participating sensing application', *Proceedings of 6th International Conference on Computer Science and Information Technology (CSIT)*, Amman, pp.166–171.

Segall, S. (2012) 'Jurisdictional challenges in the United States government's move to cloud computing technology', *Fordham Intell. Prop. Media & Ent. LJ*., Vol. 23, No. 3, p.1105.

Shastri, S., Wasserman, M. and Chidambarm, V. (2019) *GDPR Anti-Patterns: How Design and Operation of Modern Cloud-Scale Conflict with GDPR*, 31 October, pp.2–3, Cornell University.

Sordet, E. and Milchior, R. (2012) 'la définition des contours juridiques du cloud computing', *Communication, Commerce électronique*, 12 November, No. 11, pp.7–11.

Stylianou, K. (2010) 'An evolutionary study of cloud computing services privacy terms', *J. Marshall. Computer & Info. L.*, Vol. 27, No. 4, p.593.

Sub, F. et al. (2019) 'Cloud security and security challenges revisited', *Proceedings of the Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, p.61.

Tari, Z. et al. (2015) 'Security and privacy in cloud computing: vision, trends, and challenges', *IEEE Cloud Computing*, Vol. 2, No. 2, pp.30–38.

Weiss, M. and Archick, K. (2016) 'US-EU data privacy: from safe Harbor to privacy shield', *Congressional Research Service*, May, pp.1–16.

Xiao, Z. and Xiao, Y. (2013) 'Security and privacy in cloud computing', in *IEEE Communications Surveys & Tutorials*, Vol. 15, No. 2, pp.843–859, Second Quarter 2013, doi: 10.1109/SURV.2012.060912.00182.

Yang, C., Huang, Q., Li, Z., Liu, K. and Hu, F. (2017) 'Big data and cloud computing: innovation opportunities and challenges', *International Journal of Digital Earth*, Vol. 10, No. 1, pp.13–53.

Zhou, J. et al. (2015) 'Security and privacy in cloud-assisted wireless wearable communications: challenges, solutions, and future directions', in *IEEE Wireless Communications*, April, Vol. 22, No. 2, pp.136–144, doi: 10.1109/MWC.2015.7096296.