# Your digital home is no longer your castle: how cloud computing transforms the (legal) relationship between individuals and their personal records

Irion, K.

DOI
10.1093/ijlit/eav015

Publication date
2015

Document Version
Final published version

Published in
International Journal of Law and Information Technology

*International Journal of Law and Information Technology*, 2015, 23, 348–371
doi: 10.1093/ijlit/eav015
Advance Access Publication Date: 27 September 2015
Article

OXFORD

# Your digital home is no longer your castle: how cloud computing transforms the (legal) relationship between individuals and their personal records

Kristina Irion*

## ABSTRACT

In line with the overall trend individuals' personal affairs, too, are composed of digital records to an increasing amount. At about the same time, the era of local storage in end-user equipment is about to give way to remote computing where data resides on third party equipment (cloud computing). Once information, and even the most personal one, is no longer stored on personal equipment the relationship between individual users and their digital assets belonging to them is becoming increasingly abstract. This contribution focuses on the implications of cloud computing for individuals' unpublicized digital records. The question to be answered is whether—taken together—the progressing virtualization and the disruption of physical control produce a backslide for individual positions of rights. The article introduces the legal treatment of users' digital personal records and how a technical transformation in combination with disparate legal protection and prevailing commercial practices are bound to impact the distribution of rights and obligations.

**KEYWORDS**: cloud computing, consumers, EU law, personal records, security, control, privacy

## INTRODUCTION

In line with the overall trend towards virtualization, individuals' personal affairs, too, are composed of digital records to an increasing amount. Today, everybody keeps digital records of photos, agendas, contracts, transactions, diaries, etc., which are no longer filed away and kept as physical artefacts, visible in our homes becoming more sleek and minimalist. At about the same time, the era of local storage in end-user equipment is about to give way to remote computing where data resides on third party equipment.

* Marie Curie fellow, Institute for Information Law, University of Amsterdam, Korte Spinhuissteeg 3, Amsterdam, Netherland; Associate Professor, School of Public Policy, Central European University, Nador utca 9, Budapest, Hungary. E-mail: k.irion@uva.nl.
The research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA grant agreement ñ PIEF-GA-2012- 327916.

Untying users' personal records data from the hardware essentially facilitates users' mobility who can now access their information across multiple devises. This trend is reinforced by a new hardware generation thin clients that are designed to seamlessly interact with virtual capacity at a remote location. Individual consumers migrate to cloud-based services that are offered to them by their devise manufacturer or service provider, ready to use and in the most basic version even free of charge. This is modern, this is the future and in some aspects this is beneficial for individuals being relieved from cumbersome backing-up procedures and data losses from hardware failure for example. However, once information, and even the most personal one, is no longer stored on personal equipment the relationship between individual users and the digital assets belonging to them is becoming increasingly abstract.

This contribution focuses on the implications of cloud-based services for individuals' digital personal records which used to sit on our desktop but are now in the custody of a third party.[1] The question to be answered is whether—taken together—the disruption of physical control and cloud services' commercial propositions produce a backslide for individual positions of rights that is not properly understood. This article introduces the legal treatment of users' unpublicized data at rest in the cloud and how a technical transformation in combination with disparate legal protection and prevailing commercial practices are bound to impact individuals. As information can be subject to various legal regimes this legal patchwork is likely to produce disparate levels of protection and even gaps where no protection is afforded. The issue is arguably reinforced by commercial practices that favour the service provider as a result of which individual users are likely to be the most disenfranchised.

Despite of the growing body of legal literature on cloud computing the particular angle of individual consumers' personal records residing in cloud-based services has received only very sporadic attention. A large body of legal research and policy documents on cloud computing discusses business consumers as cloud clients as a reflection of the economical relevance of business-to-business transactions.[2] For that matter, individuals as end users of cloud computing are facing different legal issues compared to organizations and businesses. The remainder of the literature shows how sector-specific laws would apply in situations where individual users provision themselves with cloud services. Notably, the QMUL Cloud Legal Project[3] conducted relevant legal research in relation to cloud computing and its outputs contribute

1 The disclosure of personal information on social media and the wider phenomenon of user-generated content that is published online are not considered.

2 Art 29 Data Protection Working Party, 'Opinion on Cloud Computing, WP 196' (2012) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf> accessed 24 March 2014; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Unleashing the Potential of Cloud Computing in Europe' (2012) <http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf> accessed 7 April 2014.

3 The QMUL Cloud Legal Project's website is available at <http://www.cloudlegal.ccls. qmul.ac.uk/> accessed 19 June 2015, the successor of which is the Microsoft Cloud Computing Research Centre (MCCRC) available at <http://www.mccrc.eu/> accessed 19 June 2015.

important pieces to the legal puzzle. Apart from contract law[4] the sector-specific regimes pertaining to data protection[5] and consumer protection[6] in the European Union (EU) have received much scholarly attention. This research takes a unique perspective when exclusively focusing on individual consumers as cloud users and assessing the transformational impact of cloud sourcing on individual consumers' information's legal protection.

The article proceeds as follows: it first lays the basis for understanding the transformations personal record-keeping practices have undergone that culminate now in individual consumers increasingly using cloud services. In a next step consumer-facing cloud services are briefly introduced covering, inter alia, demand and supply factors. Against this backdrop the issues of security, control and privacy receive attention from the perspective of individual consumers of cloud services which is contrasted with the contractual arrangements that characterize consumer-facing cloud computing today. The article then turns to legal protections afforded in EU law to individual consumers' personal records in the custody of the cloud service providers before presenting notable policy initiatives at the EU level followed by the conclusion.

## THE TRANSFORMATION OF PERSONAL RECORD KEEPING

In order to set the scene this section briefly introduces the notion of personal records before it considers the transformations personal record-keeping practices have undergone. Every individual holds a variety of personal records for private purposes that fulfil different functions in private life. These functions can be broadly distinguishedin, on the one hand, personal documentation and management, and on the other hand, ideational items and intellectual explorations in the widest sense.[7] Under the first category fall copies of certificates (eg birth, IDs), other biographical records (eg education and employment history), copies of contracts and transactions and also personal agendas, for example. The second category assembles private memories and other content (eg diaries, private correspondence and images), and the output and input of intellectual explorations (eg creative expressions, personal libraries of books, music and films). Obviously, there is no uniform collection of

4 Simon Bradshaw, Christopher Millard and Ian Walden, 'Standard Contracts for Cloud Services' in Christopher Millard (ed), *Cloud Computing Law* (OUP 2013) 39–72; Phillipe Marchandise, 'Cloud Computing - Overeenkomsten En de Aansprakelijkheid van Cloud Service Providers' (2014) 4 Cah Jur 101 <http://nl.bruylant.larciergroup.com/resource/extra/9782802749516/Cahier du juriste 2014 4 extr.pdf> accessed 10 June 2015; DLA Piper UK LLP, 'Comparative Study on Cloud Computing Contracts. Final Report' (2015) <http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/> accessed 10 June 2015.

5 W Kuan Hon, Christopher Millard and Ian Walden, 'What is Regulated as Personal Data in Clouds?' in Millard, ibid 167–92; W Kuan Hon, Christopher Millard and Ian Walden, 'Who is Responsible for Personal Data in Clouds?' in Millard, ibid 193–219; Yves Poullet and others, 'Data Protection in the Clouds' in Serge Gutwirth and others (eds), *Computers, Privacy and Data Protection* (Springer Netherlands 2011) 377–409; Joep Ruiter and Martijn Warnier, 'Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice' in Gutwirth and others ibid 361–76.

6 Alan Cunningham and Chris Reed, 'Consumer Protection in Cloud Environments' in Millard (n 4) 331–61.

7 Julie E Cohen, 'DRM and Privacy' (2003) 18 Berkeley Tech LJ 575, 576–617; Neil M Richards, 'Intellectual Privacy' (2008) 87 Texas L Rev 387, 408–45.

personal records but they differ from one to the other as a reflection of individuals' diversity.

## FROM PHYSICAL ARTEFACTS TO DIGITAL FILES AND INTO THE CLOUD

In order to appraise the transformation induced by technological progress it is helpful to pause for a moment and look back to personal records in the era of physical artefacts. Until recently, paper has by far been the predominant carrier of information in addition to other mainstream analogue storage media, such as magnetic tapes. At the end of the 20th century, in virtually every segment of life, digitalization has been transforming the way how individuals generate, obtain and keep their personal records. The conversion of any type of analogue source into binary code only describes the technical processes underlying digitalization, the transformative powers of which are deep and far reaching for society and individuals alike.

Personal computing and other digital end-user equipment produce digital personal records. Capable digital cameras that are included in smart phones and tablets and also available as stand-alone devises are mainstream consumer equipment today with which individuals generate massive amounts of digital images and videos.[8] Books, music and movies are now digital content that is licensed to individuals for personal use instead of acquiring property of the chattel.[9] Standard application software on personal computers, such as a word editor or a spreadsheet software, supports individuals in many activities of their personal life as a private user, citizen and consumer. New applications, such as agendas, contact lists and other utile functionalities diversify the reliance on digital methods to personal organization.

The step from digital records to cloud computing is closely linked to the latest evolution of personal computing[10] that is characterized by the centralization of computing power away from local hardware clients.[11] The cloud epithet is used as shorthand to describe a computing model where storing, processing and use of data takes place on remotely located computers accessible over the Internet.[12] This article does not attempt to convey the complex technological background of cloud technology which has been accomplished elsewhere.[13] For now it suffices to

8 Gartner, 'Gartner Says That Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016' (Stamford, Conn, 2012) *Press Release* <http://www.gartner.com/newsroom/id/2060215> accessed 10 June 2015.

9 Natali Helberger and others, *Digital Consumers and the Law. Towards a Cohesive European Framework* (Bernt Hugenholtz ed, Wolters Kl 2013) 3.

10 Michael R Nelson, 'The Cloud, the Crowd, and Public Policy' (2009) 25 Issues Sci Technol <http://issues.org/25-4/nelson-2/> accessed 10 June 2015; cf Poullet and others (n 5) 379.

11 Kenji E Kushida, Jonathan Murray and John Zysman, 'Diffusing the Cloud: Cloud Computing and Implications for Public Policy' (2011) 11 J Ind Compet Trade 209–37.

12 European Commission (n 2).

13 Michael Armbrust and others, 'Above the Clouds: A Berkeley View of Cloud Computing Cloud Computing: An Old Idea Whose Time Has (Finally) Come' [2009] Technical Report No UCB/EECS-2009-28 <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf > accessed 10 June 2015; Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing - SP800-145.pdf' (2011) NIST SP 800-145 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf> accessed 8 April 2014; W Kuan Hon and Christopher Millard, 'Cloud Technologies and Service' in Millard (n 4) 3–17; Armbrust and others (n 13).

understand that as a consequence of a wider technological paradigm shift personal records too started to migrate from local hardware to online storage and individuals can now use online applications instead of locally installed software.

What is of interest to this research is not primarily the generative change of the format in which information are captured, but how the transformation to remote computing impacts on the relationship between individuals and their digital personal records. Even though a carrier medium and therefore physical infrastructure remains necessary, information today can behave ephemeral and volatile. What used to reside in the domestic sphere is now detached from its source and can now even live outside of personal hardware and physical spheres of influence. However, social practices and legal norms were evolving against the backdrop when information were annexed to a chattel not anticipating the abstraction induced by the move towards remote computing.[14]

## CONSUMER-FACING CLOUD SERVICES

Several mutually reinforcing trends stimulate the take-up of consumer-facing cloud services. Cloud-based storage, also known as online backup service, offers an easy means to come to terms with consumers' growing storage needs, mainly due to digital photography and video.[15] In 2014, a Eurostat survey found that already a fifth of the EU population made use of cloud storage to save files of pictures, documents, music, videos or others.[16] According to an industry forecast, by 2018 more than 79 per cent of Western European Internet users will use cloud-based storage compared to only 39 per cent of Internet users in Central and Eastern Europe.[17] It is estimated that by 2016 consumers will be storing a third of their digital content in the cloud, which is up from just 7 per cent in 2011.[18]

As a benefit, consumer-facing cloud services reduce one-off costs for hardware and software licenses; in many instances their cloud-based equivalents are as a basic version even free of charge.[19] The vast majority of EU users, ie 88 per cent, today sign-up for free cloud-based storage, only 1 in 10 users opts for paid

14 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harv L Rev 193–220 <http://www.jstor.org/stable/1321160> accessed 4 March 2015; Bert-Jaap Koops, 'On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy' [2014] Politica & Società 1–18 <http://www.rivisteweb.it/doi/10.4476/77102> accessed 4 March 2015.

15 The average storage per household is expected to increase from 464 gigabytes in 2011 to 3.3 terabytes in 2016, cf Gartner (n 8); Civic Consulting, 'Cloud Computing. Study Prepared for the European Parliament's Committee on Internal Market and Consumer Protection' (2012) 19 <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_EN.pdf> accessed 24 March 2014.

16 The highest proportions of individuals using cloud services were found in Denmark (42%), UK (38%), Luxembourg and Sweden (35%) and the Netherlands (34%). At the lower end, fewer than 1 in 10 individuals in Poland, Lithuania and Romania used cloud services for saving files. Heidi Seybert and Petronela Reinecke, 'Half of Europeans Used the Internet on the Go and a Fifth Saved Files on Internet Storage Space in 2014' [2014] Statistics in Focus 3 <http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_and_cloud_services_-_statistics_on_the_use_by_individuals>.

17 Cisco, 'Cisco Global Cloud Index: Forecast and Methodology, 2013–2018' (2013) 39 <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf> accessed 10 June 2015.

18 Gartner (n 8).

19 Eg Dropbox offers 2 gigabyte for free, Apple iCloud 5 gigabyte, Microsoft's OneDrive and Google Drive 15 gigabyte, see Emma Lunn, 'Cloud Sourcing: Which Remote Storage Should You Choose?" *The*

services.[20] This is possible because the individual capacity needs of consumers are still comparatively small whereby cloud technology slashes the costs of supply. For service providers it is commercially viable to operate a freemium business model on part of the cloud-based storage in order to attract individual consumers to their platform or as an add-on to online services.

Other consumer-facing online services provide functionalities that facilitate the creation and processing of personal records. Such is the case with remotely hosted standard application software that is taking over from similar applications that used to run on local hardware. The 2014 Eurostat survey finds that 12 per cent of the EU population use online software for editing text, spreadsheets or presentations.[21] With 23 per cent young people aged between 16 and 24 years are more avid users of such online software.[22]

The other compelling feature of cloud computing is that it facilitates access to services and data across multiple connected devices.[23] In Western Europe, a consumer and Internet user has an average of six devices which is why the ability to sync the same content and deliver personalized services across multiple devices is crucial.[24] This is why new generation consumer equipment, operating systems and online services increasingly integrate cloud computing into their systems and service platforms.[25] This development goes hand in hand with radically reduced local storage capacity of end-user devices, creating so-called thin clients that function like windows to applications and content, and thus need to interoperate with the cloud.[26] Thin clients that are often much cheaper than their thick counterparts are thus further diffusing individual consumers' cloud computing.[27]

## INDIVIDUAL CONSUMERS' INTERESTS AFFECTED BY CLOUD SOURCING

In sheer numbers individual users are certainly the largest group that is already directly (eg consumer cloud storage) or indirectly (eg web-based standard application software) serviced with cloud computing. As individual consumers, they are using online services downstream of cloud computing infrastructure that are conceived for mass-market adoption and offer a ready-to-use functionality.[28] Hence, individual end

*Guardian* (2014) <http://www.theguardian.com/money/2014/jan/16/cloud-storage-which-provider> accessed 7 April 2014.

20 Seybert and Reinecke (n 16) 5.

21 ibid 7.

22 Primavera De Filippi, 'Cloud Computing: Analysing the Trade-off between User Comfort & Autonomy' (*Internet Policy Review*) <http://policyreview.info/articles/analysis/cloud-computing-analysing-trade-between-user-comfort-autonomy> accessed 7 April 2014.

23 ibid.

24 Cisco (n 17) 39; Anon, 'Personal Technology: Consumerisation: The Power of Many' [2012] *Economist* 65 <www.economist.com/node/21530921> accessed 10 June 2015.

25 Eg Microsoft OneDrive comes preinstalled on Windows 8.1 and iCloud is preinstalled on iOS run apple devices.

26 Eg Google's Chromebook has almost no local storage but is marketed with 100 gigabyte of cloud storage in Google Drive. Cf Jonathan Zittrain, 'Lost in the Cloud' *The New York Times* (New York, 2009) 18 <http://www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=2&> accessed 10 June 2015.

27 Especially laptops, tablets and smart phones retail prices increase with the amount of local storage.

28 Individual consumers are the high end of the cloud service model, ie Software-as-a-Service (SaaS). This is also the case for basic consumer cloud storage because it comes with a user interface and the functionality to manage files, among other features. cf Civic Consulting (n 15) 19; Hon and Millard (n 13) 4 in fn 12.

users are not concerned with the underlying resources which are managed by the service providers, respectively. What this implies for the position of individual consumers to preside over the personal records belonging to them is examined further below. In the literature security, control and privacy are frequently raised issues with cloud computing, which are also reflected in empirical research.[29]

A 2011 survey of US consumers found that half of all respondents shared some level of concern about who owns the data in the cloud and just below 40 per cent about security and privacy of the data.[30] Likewise European consumers are concerned about privacy and security of cloud sourcing according to aforementioned Eurostat survey which can amount to a barrier for take-up of consumer-facing cloud services.[31] From those individuals who use the Internet but not cloud services even though they are aware of such services, 44 per cent cited concerns about privacy and security for their abstinence from cloud-based services.[32] But also for individual users of cloud services privacy, security and data location remain their main concerns (43 per cent) according to a different survey of 2012.[33]

The following sections on security, control and privacy offer some background of the multifarious issues and risks for individual consumers of cloud services. It should be noted, however, that these issues are somewhat overlapping since security, control and privacy are jointly tackling how individual consumers can retain the primacy over their own personal records when they are residing in the cloud.

## Security

As with any information handling technology there are a range of specific security risks associated with cloud computing which can affect individual consumers' personal records. Not all risks are new, eg hardware failure and malware, and they may actually decrease when individuals rely on cloud services which are in general better versed with technical security.[34] New risks, however, arise in the sphere of the service

29 Primavera De Filippi and Smari McCarthy, 'Cloud Computing: Centralization and Data Sovereignty' <http://ejlt.org//article/view/101/234> accessed 24 March 2014; W Kuan Hon and Christopher Millard, 'Control, Security, and Risk in the Cloud' in Millard (n 4) 18–36; Nancy J King and T Raja, 'What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data' (2013) 50 Am Bus LJ 413–82; Timothy D Martin, 'Hey - You - Get off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing' (2010) 92 J Pat Trademark Off Soc'y 283–314 <http://0-www.heinonline.org.polar.onu.edu/HOL/Print?collection=journals&handle=hein.journals/jpatos92&id=288> accessed 7 April 2014; Wolter Pieters, 'Security and Privacy in the Clouds: A Bird's Eye View' in Gutwirth and others (n 5) 445–57.

30 Ipsos OTX Media CT, 'Head in the Clouds? Cloud Computing & Consumers' [2011] *Free year-round insights Technology Edition No 2* <http://www.ipsos.com/mediact/sites/ipsos.com.mediact/files/pdf/Head in the clouds.pdf> accessed 10 June 2015.

31 Seybert and Reinecke (n 16) 6.

32 ibid.

33 IDC, 'Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-Up. Final Report. Study Prepared for the European Commission' (2012) 27 <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1115> accessed 18 February 2015.

34 Valentina Pop, 'Cloud Providers Warn against EU 'over-Regulation'' (*EU Observer*, 2011) <https://euobserver.com/cyber/113871> accessed 5 March 2015; Randal C Picker, 'Competition and Privacy in Web 2.0 and the Cloud' (2008) 414 University of Chicago Law & Economics, Olin Working Paper 6 <http://papers.ssrn.com/abstract=1151985> accessed 27 June 2014.

provider when using cloud-based services. Risks of cloud computing are commonly assessed through the lens of the information security triad, ie which risks would affect the confidentiality, the integrity or the availability of the data residing in the cloud.[35] They could be compromised not only by accident, human error or a malicious attack but also in the event of a cloud service provider's exit.

Instead of exercising a full risk assessment some examples can illustrate best the specific risks of cloud computing that are external to consumers.[36] Service outages for instance temporarily affect the availability of access to the data and unsaved data may get lost.[37] The most critical node for security, however, is the authentication mechanism through which cloud clients can effectuate remote access to their data.[38] In the recent past, many popular cloud services had to admit that their authentication was breached which had led to the adoption of more secure authentication mechanisms. Public awareness of cloud security risks certainly surged when in 2014 personal images of celebrities leaked online which hackers could obtain from a public cloud storage service.[39]

Much less known are so-called colocation risks which arise from multiple clients' sharing the same infrastructure in a public cloud.[40] In technical terms, this is called multi-tenancy which offers a good image for the colocation of many clients' data that characterizes many consumer-facing cloud services today.[41] Colocation risks can be realized as a failure to isolate a client's data from other users, thus compromising confidentiality.[42] But also in other contexts, different client's accounts, which share the same (virtual) infrastructure, may be affected by a summary approach, for example public authorities seizing infrastructure or ordering the shutdown of a service.[43]

35 cf ENISA, 'Cloud Computing Risk Assessment' (2009) <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment> accessed 7 April 2014.

36 With the exception of a user compromising her authentication credentials or wrongly instructing the service.

37 Marcus Wohlsen, 'Dropbox and Uber: Worth Billions, But Still Inches From Disaster' [2014] *WIRED* <http://www.wired.com/2014/01/dropbox-uber/> accessed 10 June 2015.

38 GF, 'Internet Security: Slack in the Box' [2012] *Economist* <http://www.economist.com/blogs/babbage/2012/08/internet-security-0> accessed 10 June 2015.

39 Tim Bradshaw, Hannah Kuchler and Sally Davies, 'Apple Admits Celebrity Accounts Hacked but Denies iCloud Breach' *Financial Times* (2 September 2014) <http://www.ft.com/intl/cms/s/0/916d7d24-327e-11e4-93c6-00144feabdc0.html#axzz3U4NwgVL7> accessed 10 June 2015.

40 Typically, individual end users rely on public cloud services in which the infrastructure is shared among clients whose data is only logically comparted from another.

41 cf Hon and Millard (n 13) 13.

42 Bianca Bosker, "Dropbox Bug Made Passwords Unnecessary , Left Data At Risk For Hours" *Huffington Post* (2015) <http://www.huffingtonpost.com/2011/06/21/dropbox-security-bug-passwords_n_881085.html> accessed 10 June 2015; Massimo Felici and others, 'Bringing Accountability to the Cloud: Addressing Emerging Threats and Legal Perspectives' in Massimo Felici (ed), *Cyber Security and Privacy* (Springer Press 2013), 32; Martin (n 29) 304.

43 Eg the seizure of a server in the context of tax law enforcement in Norway, cf *Bernh Larsen Holding AS and others v Norway* (ECHR, 14 March 2013); the wholesale deletion of individual users' (legal) data following the forced shutdown of the file sharing website Megaupload, Jon Brodkin, 'Kim Dotcom: Megaupload Data in Europe Wiped' [2015] *Ars Technica* <http://arstechnica.com/tech-policy/2013/06/kim-dotcom-megaupload-data-in-europe-wiped-out-by-hosting-company/> accessed 10 June 2015.

## Control

When individuals store or create personal records in cloud-based services this inevitably produces arrangements in which control over the data is shared between the individual and the service provider. The service provider who has effectively moved in between the individual and her data is now in the position to intermediate this relationship. At its most basic, when personal records reside with a third party and bare of any means of physical control an individual's relationship vis-à-vis her data is now abstract.[44] All control and verification is derived from the service provider.[45] A client can, for example, instruct the service to delete data but cannot influence how thoroughly this is executed, which depends on the implementation by the service provider.[46] Typically, a client of public cloud services would not know the actual location of the data nor how many copies there are.[47] Let alone that any control is highly transient given the dynamic use of cloud computing capabilities.[48]

Policy literature and some authors frame the cloud users' loss of control as a problem of 'information ownership' or 'data sovereignty'.[49] In the context of individual consumers of cloud services there are certain overlaps with the privacy interest discussed below, but in addition connoting that the user to whom the data belongs should ultimately be in control. Conceptually though, both, 'information ownership' and 'data sovereignty' are not recognized in the law and widespread perceptions of property and ownership on part of the users do not find a corresponding legal basis.[50] Nonetheless, it signals a possible gap between the intuitive perceptions of an allocation mechanism that would assign rights over the data belonging to the user of cloud services to the user. In truth, however, much of the exact arrangements depend on the contract between the cloud service provider and the individual consumer which is further elaborated below.

A sensitive moment for exercising control over the data arises whenever a service relationship ends no matter if this happens planned or unexpected. In the case of a bankruptcy or following the termination of a cloud-based service by the provider the ability to recover the data on part of the individual client may be thwarted.[51]

44 Abstract (adj) 'Existing in thought or as an idea but not having a physical or concrete existence', cf OED online, 'Abstract, Adj. and N.' (*Oxford English Dictionary*, 2014) <http://www.oed.com/view/Entry/758?rskey=tdR2Nx&result=1&isAdvanced=false> accessed 10 June 2015.

45 Art 29 Data Protection Working Party (n 2) 5; ENISA (n 35) 9; De Filippi and McCarthy (n 29); Mell and Grance (n 13) 2; Dan Svantesson and Roger Clarke, 'Privacy and Consumer Risks in Cloud Computing' (2010) 26 CLSR 391–97.

46 cf art 29 Data Protection Working Party (n 2)12.

47 The actual whereabouts of the data, however, matter for the applicability of domestic law and determining jurisdiction; cf 'The information [ . . . ] is stored temporarily on servers whose state of location is unknown, that being kept secret for reasons of competition', Case C–131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (CJEU, 13 May 2014) para 43.

48 Cloud computing supply chains can comprise of several layers and sub-providers can be dynamically added. cf art 29 Data Protection Working Party (n 2).

49 European Commission (n 2) 5; Filippi and McCarthy (n 29) 9f; Chris Reed, 'Information "Ownership" in the Cloud' 1 <http://papers.ssrn.com/abstract=1562461> accessed 6 April 2014; Chris Reed and Alan Cunningham, 'Ownership of Information in Clouds' in Millard (n 4) 142–64.

50 Reed, ibid 1.

51 Eg Deborah Gage, 'Nirvanix Files for Chapter 11 Bankruptcy' *The Wall Street Journal* (2013) <http://blogs.wsj.com/digits/2013/10/02/nirvanix-files-for-chapter-11-bankruptcy/> accessed 10 June 2015.

Without a reasonable data preservation period individual clients risk to forego the ability to retrieve their data before it is erased.[52] Another unresolved issue is how cloud clients can move data from one service provider to another. Data portability is not a standard feature of consumer-facing cloud services today which can render migrating the data to a new service a very laborious task. Individuals thus risk lock-in of their data with a service provider which can effectively limit their ability to switch to another service provider.[53]

## Privacy

Outside of protecting against security breaches the intermediation by the service provider can pose new risks of intrusion into individual consumers' privacy. Even though individual consumers' also use cloud-based services to share content with others they expect their service provider to respect the privacy of their content. Unfortunately, most surveys do not differentiate the privacy concern emanating from the intra-service relationship from situations that are more broadly characterized as security breaches. For the time being, most providers' consumer cloud storage services limit themselves to processing the individual consumers' content insofar as it is necessary to render the service, but retain certain rights to access and use necessary to comply with legal requirements.

This situation may, however, evolve subject to service providers' commercial interests and as far as legally permissible. Essentially, consumer-facing cloud services could share the faith with other popular online services in which the commodification of individuals' data is much further progressed.[54] Some authors warn against the risk of exploitation of cloud-sourced data of individual consumers especially at the onset of big data applications.[55] The question thus arises to what extent EU individual consumers would be protected under the law against disenfranchising commercial practices of cloud service providers.

From what was described above when confronted with any of these risks for their data residing in the cloud, individual end users are not very well positioned to act without the service provider. It must be conceded that the potential security risks could be outweighed by the relative security advantages of cloud-based services. By contrast, individual consumers' control and privacy interests are clearly a function of the operations and commercial practices of the cloud service provider. Contractual arrangements that are biased to unilaterally favour the service provider would only compound the issues with control and privacy in consumer-facing cloud services. The next section reviews how in view of the commercial practices today rights, obligations and risks are allocated between the individual consumer and the provider.

52 ibid; Brodkin (n 43).

53 In a freemium culture 'locking-in users to one particular online platform is key' (Alan Cunningham, 'Caveat Consumer? – Consumer Protection and Cloud Computing – Part 1' [2013] SSRN Electronic Journal 3 <http://papers.ssrn.com/abstract=2202758> accessed 24 March 2014) in order to generate revenue at the back of the service, eg with online advertisement.

54 cf Cunningham and Reed (n 6); William Jeremy Robinson, 'Free at What Cost?: Cloud Computing Privacy' (2010) 98 Georgetown LJ 1195–239.

55 Vincent Mosco, *To The Cloud. Big Data in a Turbulent World* (Paradigm 2014) 179; Picker (n 34) 3.

## CLOUD SERVICE CONTRACTS FOR INDIVIDUAL CONSUMERS

The contract between the service provider and individual consumer that governs the cloud service relationship is commonly referred to as terms of service. The terms of service are binding between the parties and allocate responsibilities and rights in respect of the service.[56] Albeit the terms of service of consumer-facing cloud offerings by different service providers are diverging in detail, there are a number of commonalities where commercial practices are converging. Important differences, however, can stem from the relevant jurisdiction and regulatory framework in which a specific cloud service operates.

The terms of service can work two ways: where they place adequate contractual obligations on the service provider they can be a means to mitigate the risks associated with cloud computing and produce a fair allocation of rights and responsibilities. Conversely, the terms of service can also be used to exclude as much as possible the service provider's liabilities and responsibilities, including certain regulatory obligations insofar as they can be written-off or manipulated to better correspond with the interest of the service provider.[57] In that case, the contractual arrangement would serve to reinforce the client's dependency from the service provider and thus only entrench the loss of control over her data.

### Standard terms of service

Consumer-facing cloud services are almost always subject to standard terms of service which are unilaterally stipulated by the service provider.[58] Individual consumers are prompted to accept the terms of service when they sign up for cloud services ('Take it or leave it').[59] This lack of negotiation power vis-à-vis the service provider creates an asymmetry that can be readily exploited by setting conditions to their favour, in particular, to exclude liabilities, limit obligations and restrict clients' rights.[60] Available surveys on standard terms of service of public cloud service providers confirm that it is common practice to leverage the contract as much as possible to shield the service provider from their customers' claims.[61] To the end

56 Chris Turner, *Unlocking Contract Law* (Routledge 2014) 1.1.3.

57 Lee A Bygrave, *Internet Governance by Contract* (OUP 2015) 6; Ian Walden, 'Demystifying Regulation in the Cloud: Opportunities and Challenges for Cloud Computing' (2012)12 <http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/documents/GSR12_Cloud_Walden_5.pdf> accessed 24 March 2014.

58 Bradshaw, Millard and Walden (n 4); Cunningham and Reed (n 6).

59 European Commission (n 2) 11; cf discussion about end-users' acceptance of standard terms and conditions Ellen Wauters, Eva Lievens and Peggy Valcke, 'Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites' (2014) 22 Int J L Info Technol 254–94 <http://ijlit.oxfordjournals.org/cgi/doi/10.1093/ijlit/eau002> accessed 10 June 2015.

60 European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'' (2012) 5 <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf> accessed 10 June 2015.

61 Bradshaw, Millard and Walden (n 4); Norwegian Consumer Council, 'Hazy Terms in the Cloud' (2014) <http://www.forbrukerradet.no/annet/tester-og-kjøpetips/undersøkelser/hazy-terms-in-the-cloud>.

Bradshaw, Millard and Walden observe that:

> [A] number of providers of consumer-oriented cloud services appear to disclaim the specific fitness of their services for the specific purpose(s) for which many customers will have signed-up to use them.[62]

Not only that the individual consumers bear the security risks of cloud computing that are external to them, but the service provider also retains extensive discretion during the service relationship and of its termination. In general, service providers reserve themselves the right to unilaterally change the standard terms of service either subject to advance notice but in some cases not even that.[63] In its 2014 study of the terms and conditions of seven most popular cloud storage services in Norway, the Norwegian Consumer Council criticized that one service could unilaterally change the terms of service without notice and to immediate effect and none assumed any warranty against data loss.[64] With some variations, the terms of service of the largest public cloud service providers foresee that the service can be terminated at any time without giving a valid reason.[65]

Some cloud storage services' standard terms of service make an explicit statement about the ownership over the data which they receive.[66] Nevertheless such statements should not be taken at face value to produce the effect that under all circumstances individual consumers' personal records are never accessed and used by the service provider. To the contrary, most cloud service providers do retain some rights to review users' files. To this extent the terms of service cover or link-in second-tier policies of the cloud service provider, notably the acceptable use policy and the privacy policy that carve out rights of access to and use of the consumers' data on behalf of the service provider.[67]

### Access and use rights

In practice, the terms of service of several major cloud services grant themselves a worldwide license to use the customer's data for enumerated purposes that can extend to third parties involved in the provision of the service.[68] At present, these purposes are oftentimes limited to rendering the service and to use the data to improve it, but in addition also comprises legal obligations that service providers have to comply with. Examples are removing copyright infringing content after a notice

62 Bradshaw, Millard and Walden (n 4) 52.

63 James Crisp, 'Norway Accuses Apple of Breaching EU Consumer Law' (*EurActive*, 2014) <http://www.euractiv.com/sections/infosociety/norway-accuses-apple-breaching-eu-consumer-law-302123> accessed 5 March 2015; Bradshaw, Millard and Walden (n 4) 51.

64 Norwegian Consumer Council (fn 61); Bradshaw, Millard and Walden (n 4) 58f.

65 Norwegian Consumer Council (n 61); Cunningham and Reed (n 6) 354f.

66 Eg Microsoft's general service agreement states of 11 June 2014 states: '[w]e don't claim ownership of the Content you provide on the Services' <http://windows.microsoft.com/en-us/windows/microsoft-services-agreement> accessed 20 April 2015.

67 DLA Piper UK LLP (n 4) 36f.

68 Eg Google Terms of Service of 14 April 2014 state: 'The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones.' <http://www.google.com/policies/terms/> accessed 20 April 2015; Norwegian Consumer Council (n 61).

by the rights holder and complying with disclosure authorities under applicable national laws.[69] Notwithstanding the lawful nature of such access and use rights, their existence exemplifies that the intermediation of personal records supersedes individual customers' control.

Beyond the purview of legal obligations, service providers can leverage their own interests to access and use individual consumers' personal files. In 2014, the Norwegian Consumer Council criticized two services for obtaining licenses to use the content beyond what is necessary for the operation of the service and to comply with legal obligations.[70] In one instance that covers a bundle of online services, including the provider's web email and cloud storage service, the terms of service provide for the automated analysis of the users' content for a range of purposes, including tailored advertisement.[71] Robison differentiates three distinct categories of terms of service agreements that allow varying degrees of authority over a customer's data:

1. Explicit authority to access a customer's data for marketing purposes.
2. Vague authority to access a customer's data for purposes beyond the primary services.
3. Explicit prohibitions against accessing a customer's data for any purpose other than providing a specific service.[72]

The concern would be that more consumer-facing cloud services from the bottom category could move to the top when they start mimicking the example of other popular online services. According to their business model online services are marketed as free, while consumers' information are the input for the actual revenue-making activities, predominantly through personalized online advertisement.[73] It would be relatively easy for service providers to expand the purposes for which they can

69 Microsoft's general service agreement of 11 June 2014 states: '. . . but we also deploy automated technologies to detect child pornography or abusive behavior that might harm the system, our customers, or others. When investigating these matters, Microsoft or its agents will review Content in order to resolve the issue'. Apple iCloud terms and conditions of 20 October 2014 state: 'Apple reserves the right at all times to determine whether Content is appropriate and in compliance with this Agreement, and may prescreen, move, refuse, modify and/or remove Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable.' <http://www.apple.com/legal/internet-services/icloud/en/terms.html> accessed 30 April 2015. Dropbox DMCA policy foresees taking actions in the event of copyright infringements including removal of the challenged content, <https://www.dropbox.com/terms#dmca> accessed 30 April 2015.

70 Norwegian Consumer Council (n 61); Bradshaw, Millard and Walden (n 4) 58f.

71 Eg Google Terms of Service of 14 April 2014 states: 'Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.' <http://www.google.com/policies/terms/> accessed 20 April 2015.

72 Robinson (n 54) 1195.

73 Eg the social networking site Facebook reported it has 1.39 billion active users end of 2014 and earned 12,664 billion US dollar in revenue that is mainly derived from online and mobile advertisement. Facebook, 'Facebook Reports Fourth Quarter and Full Year 2014 Results' (2015) <http://investor.fb.com/releasedetail.cfm?ReleaseID=893395> accessed 10 June 2015. The latest update of Facebook's terms, data and cookies policies which enters into force if a user logs on to the service after a deadline in January 2015 continues to expand the ability of the company to use all data is has from and about its users.

access and use clients' data through subsequent unilateral modifications of the terms of service. It is, thus, important to clarify the extent to which this is possible in EU law pertaining to data protection and consumer protection.

## Privacy policies

Privacy is an emphasized attribute of most standard terms of service and adjacent policies of public cloud services. Cloud providers' privacy policies, however, are only partially conclusive about the level of privacy they afford since they do not override the exceptions already contained in the terms of service and the acceptable use policy (and sometimes repeat them). In general, privacy policies do not create additional responsibilities in relation to the individual consumers' content received under the cloud-based service. Providers of cloud services are especially not introducing any relationship that would give rise to a fiduciary duties vis-à-vis the data it receives from clients.[74] Certain service providers' privacy policies distinguish between users' content and other personal identifiable information in connection with the use of the service which are collected and used according to different policies.[75] Other commitments, such as personal data breach notifications, are not (yet) a standard feature of consumer-facing cloud services' privacy policies.

Most contractual arrangements that are unilaterally stipulated by the cloud service providers fall short in achieving a fair balance with individual consumers' interests in security, control and privacy as outlined above. The most noticeable issues are that:

- the best effort approach in the provision of cloud-based services without minimum contractual obligations leave individual consumers to bear specific risks of cloud computing that are external to them;[76]
- individual consumers are not ascribed effective means to exercise control about essential tenets of data handling and corresponding information duties;
- the privacy of unpublicized personal records in the custody of the cloud is presently not adequately protected especially in the relationship with the service provider, notably access and use rights should be strictly limited to what is provided for by law;[77] and
- there no (post-)contractual duties that would protect individual consumers against termination by the service provider and prescribe how to orderly recover, transfer or migrate personal records and for how long this must be guaranteed for.

When cloud-based services are to replace local storage on personal consumer equipment the ensuing transformation of personal record-keeping practices should not result in less factual control and legal protection afforded to individual

74 Bradshaw, Millard and Walden (n 4) 58.

75 cf Dropbox Privacy Policy, Version of 13 February 2015, <https://www.dropbox.com/privacy> accessed 20 June 2015.

76 Cunningham and Reed (n 6) 355.

77 Where such interference with individuals' fundamental rights can be justified against the standards of European fundamental rights law, eg art 8(2) of the European Convention on Human Rights, art 7 in conjunction with art 52(1) of the EU Charter of Fundamental Rights.

consumers. While there is much focus on security in the present discussion about cloud computing what is often neglected is that service providers pursue own operational interests and commercial strategies that can accrue to fundamental concerns about individuals' privacy and control over their personal records. Especially, the terms of service cannot be left at the sole discretion of intermediaries that receive and manage unpublicized personal records on behalf of individual consumers.

The next section introduces the legal treatment of users' unpublicized data at rest in the cloud and interrogates the fitness of the legal protections afforded to individual consumers' personal records. It concisely tackles three pertinent legal regimes: copyright law, EU data protection law and consumer protection law.

## LEGAL PROTECTION AFFORDED TO PERSONAL RECORDS IN THE CLOUD

As information individuals' personal records can be subject to various legal regimes in EU and Member States' laws. Depending on the case-specific circumstances, the laws of copyright, data protection and consumer protection can apply to information in a cloud service relationship.[78] As much as possible the legal situation is covered against the backdrop of EU secondary law albeit in order to apply the relevant Directives have to be first transposed into Member States' national laws.[79]

### Copyright law

Individual consumers' digital images and videos, writings and other own creations in digital format can be works that receive copyright protection. However, whether a particular work qualifies for protection is a matter of Member States' copyright laws subject to national requirements that vary in some respects quite significantly.[80] Provided that certain personal records generated by individual consumers would indeed qualify as copyright protected works they are protected from unauthorized uses. The author can exercise a range of exclusive rights which are harmonized by Directive 2001/29/EC (EU Copyright Directive).[81]

Most service providers are cognizant of users' intellectual property rights and their terms of service clarify that cloud sourcing copyright protected works does not alter the ownership status of the author. Nevertheless, the standard terms of service are generally also conceived as conferring licenses to perform various acts the author of the work has agreed to when signing up for the service. Certain licenses so acquired are quite expansive where they authorize quasi-unlimited uses, apply worldwide and outlive the service relationship.[82] It follows that even under the privileged

78 Cunningham and Reed (n 6); Hon, Millard and Walden (n 5); Reed and Cunningham (n 49).

79 cf art 288 of the Treaty on the Functioning of the European Union (consolidated version), [2012] OJ C 326.

80 Cunningham and Reed (n 6) 145.

81 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, [2001] OJ L 167, 10–19.

82 Eg Google Terms of Service of 14 April 2014 state: 'When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (...), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited

circumstances that certain personal records are copyright protected this does not prevent these works from being subjected to a wide range of access and use rights under the service providers' terms of service. Under copyright law, contracts of adhesion are a perfectly acceptable means of authorizing the use of copyright protected works.

It should be noted that individual consumers also make use of copyright protected works of third parties, as for example would be the case for digital books, music and videos, the use of which ideally requires a license from the copyright owner. In this situation, individual consumers of cloud services are not in the position to issue sub-licenses to the cloud service provider and the cloud sourcing as well as any access and use rights should comply from the outset with relevant copyright laws. This is another legal challenge for cloud computing that is outside the scope of this article but discussed elsewhere.[83]

## Data protection law

In order for EU data protection law to afford protection a chain of legal condition must be met. Notably, the data processing in question has to fall inside the scope of application and the cloud service provider should qualify as the controller in the relationship with an individual consumer of a cloud service. Where it applies, EU data protection law places a range of obligations on the controller and individual cloud consumers can invoke data subject's rights. The pending reform of EU data protection law would introduce some important changes in the context of consumer cloud services.

### *Scope of application*

Personal records of individual cloud customers are certainly protected subject matter under EU data protection law pursuant to Directive 95/46/EC (Data Protection Directive).[84] Whether, however, a particular consumer-facing cloud service is falling within the scope of application of the EU Data Protection Directive depends on whether either criteria of its article 4 is met. In order for EU data protection law to apply the cloud service provider has to be established on the territory of a Member State (article 4(1)(a) of the Data Protection Directive) or, where this is not the case, makes use of data processing equipment situated on the territory of a Member State (article 4(1)(c) of the Data Protection Directive). Since cloud services can operate globally some providers which are established outside of the EU territory and do not make use of any data processing equipment within would not be covered by the scope of application of the Data Protection Directive.[85]

purpose of operating, promoting, and improving our Services, and to develop new ones.' <http://www.google.com/policies/terms/> accessed 20 April 2015.

83 Reed and Cunningham (n 6) 153f.

84 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 31–50.

85 However, note that the CJEU has interpreted art 4(1)(a) of the EU Data Protection Directive to apply to controllers with an establishment situated in a Member State whose activities are inextricably linked to the data processing activities of the controller, *Google Spain SL* (n 47) paras 56, 60.

In addition, individual consumers of cloud services would certainly qualify for the so-called household exemption under the Data Protection Directive. Article 3(2) provides that this Directive shall not apply to the processing of personal data by 'a natural person in the course of a purely personal or household activity'. This in turn raises the question whether instead the cloud service provider can be considered the controller of the personal data it receives from individual consumer. This is not evident across all consumer-facing cloud service providers. While cloud-based application software and the processing of personal data for secondary purposes,[86] such as marketing, would trigger the controller definition, providers of mere cloud-based storage may presently escape the Data Protection Directive.

The latter could be deemed not to be controllers because providing cloud-based storage even on request of individual consumers can fall short of the definition in article 2(d) of the Data Protection Directive according to which it is the controller who determines the purposes and means of the processing of personal data. In the context of business-to-business cloud service relationships, the article 29 Working Party, in its 2012 opinion on cloud computing, designates cloud customers as controllers and service providers as processors even where standard terms of service imply an imbalance of negotiation power.[87] This would, however, result in somewhat paradoxical situation that in order for personal records of individual consumers to be protected by EU data protection law the provider has to process the personal data for other purposes in addition to rendering the cloud storage service.

### *Obligations of the controllers*

In those situations in which EU data protection law applies all personal data processing activities must comply with a set of principles (article 6 of the Data Protection Directive) and meet either criteria of article 7 of the Data Protection Directive that render the processing legitimate. Aside from rendering the very cloud service, all additional access and use rights foreseen in the standard terms of service have to meet a legitimate ground for processing personal data. The controller can, for example, invoke article 7(c) of the Data Protection Directive that permits the processing where it 'is necessary for compliance with a legal obligation to which the controller is subject' as a legal basis for compliance with disclosure authorities and copyright enforcement actions.

Accessing and using personal records for other secondary purposes, such as marketing and tailored advertisement, could however only take place if individual consumers have given their unambiguously consent (article 7(a) of the Data Protection Directive). Article 2(h) of the EU Data Protection Directive defines consent as 'any freely given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed'. Access and use rights provided for in the cloud service providers' standard terms of service and the privacy policies to which the individual consumer has agreed would not be considered to meet the definition of consent under the Directive. A consent that forms a legitimate basis for personal data processing for secondary purposes would require an opt-in by the individual consumer.

86 Art 29 Working Party (n 2) 8.
87 ibid.

It is worth highlighting that the personal data contained in individual consumer's cloud service can include special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of data concerning health or sex life. Article 8 of the Data Protection Directive provides for much stricter requirements for the lawful processing of such special categories of personal data. For many consumer-facing cloud services it can be difficult to ascertain from the outset that individual consumers' personal records do not contain any special categories of personal data.

### *Data subjects' rights*

At the first glance, data subject's rights provided for in article 12 of the Data Protection Directive do not correspond well to the situation of consumer-facing cloud services.[88] Accordingly, data subjects can request from the controller information about the processing of their personal data and demand the rectification, erasure or blocking of personal data, for example where it is incomplete or inaccurate. The right to erasure alone is meaningful in the event of individuals wishing to remove their digital records from a given cloud service. However, without a right to data portability individuals' ability to move their content to another cloud service provider is thwarted. The Data Protection Directive does not confer individuals a right to instruct the service provider which would compensate for the loss of control nor does a duty of confidentiality arise in the relationship between service provider and individual consumer.

### *Data protection reform*

The ongoing legislative procedure for a new EU General Data Protection Regulation that is expected to be passed this year may eventually bring some relief.[89] The scope of application would be expanded to cover controllers or processors even when they are not established in the Union, where their processing of personal data relates to the offering of goods or services to data subjects in the EU, or the monitoring of such data subjects. For the finding that a good or service is offered to data subjects in the EU it would not matter whether a payment of the data subject is required. In other words, the pervasive freemium online services are also unquestionably covered under the new regulation.

Moreover, the draft clarifies that the household exception should not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities. It was noted that this clarification is important in relation to providers of cloud services for consumers who should not benefit indirectly from the 'household exception'.[90]

88 Dimitra Kamarinou, Christopher Millard, and W. Kuan Hon, 'Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers' Queen Mary School of Law Legal Studies Research Paper No. 209/2015 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646447> accessed 14 September 2015.

89 cf the legislative proposal of the European Commission for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final. Available at <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 20 June 2015.

90 Opinion of the European Data Protection Supervisor (n 60) para 39.

Last but not least, the new regulation could bring about a right to data portability under which data subjects can request to receive all personal data, which he or she has provided to a controller, and have the right to transmit those data to another controller.[91] Data portability if passed in the new regulation is bound to become a crucial right for individual consumers who wish to leave with their personal records a cloud service provider or migrate to another service provider. According to the latest Eurobarometer survey, two-thirds of the respondents agreed that the right to data portability is very or fairly important.[92] Such right would ultimately help reduce factual customer lock-in with a particular cloud service provider and in doing so stimulate competition between different consumer-facing cloud services. This in turn can actually contribute to raising the bar for freemium services in terms.

## Consumer protection law

The body of EU consumer protection law which can apply to different aspects of consumer-facing cloud services comprises three Directives: the Unfair Terms Directive (93/13/EEC) pertaining to consumer contracts,[93] the Unfair Commercial Practices Directive (2005/29/EC)[94] and the recent Consumer Rights Directive (2011/83/EC).[95] These rules are mandatory, thus standard terms of service cannot derogate from EU consumer protection law where applicable.[96] In addition, the E-Commerce Directive (2000/31/EC)[97] is to be mentioned although it protects all customers of information society services and not just consumers.

### *Scope of application*

In order for the Unfair Terms Directive and the Consumer Rights Directive to apply, the standard terms of service must qualify as a contract with a consumer. Since this article's focus is on individual consumers' personal records in cloud-based service, the EU definition of consumer would be met.[98] It should be noted, however, that

91 For background cf Eleni Kosta and others, 'Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation' (2014) 172 Queen Mary University of London, School of Law, Legal Studies Research Paper 44 <http://ssrn.com/abstract=2405971> or <http://dx.doi.org/10.2139/ssrn.2405971> accessed 10 June 2015.

92 TNS Opinion & Social, 'Special Eurobarometer 431: Data Protection', vol 431 (2015) 42 <http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf> accessed 10 June 2015.

93 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95/1993, 29–34.

94 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, OJ L 149/2005, 22.

95 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, OJ L 304/2011, 64–88.

96 DLA Piper UK LLP (n 4) 29.

97 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178/2000, 1–16.

98 The definition of consumer is identical in both, the Consumer Rights Directive (art 2(1)) and the Unfair Terms Directive (art 2(b)): '"consumer" means any natural person who, in contracts covered by this Directive, is acting for purposes which are outside his trade, business, craft or profession'.

there are quite a few ambiguous situations when individuals are pursuing commercial or mixed activities.[99] In this respect, Member States' national laws differ with some also being applicable to business-to-business contracts and mixed uses.[100]

Provided that the large majority of individual consumers of cloud services populate free services, the question arises whether free services are inside the scope of application of the EU consumer protection law and the e-Commerce Directive. EU consumer protection law incorporates the notion of a contract concluded between a trader or seller and a consumer (article 1(1) of the Unfair Terms Directive; article 3(1) of the Consumer Rights Directive). This may actually conflict with the contract law in some Member States which require an exchange taking place between the supplier and the consumer. The Unfair Terms Directive applies to the standard terms of service of cloud services irrespective of whether the consumer pays a price or not.

The e-Commerce Directive defines an information society service as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (article 2(a) of the e-Commerce Directive in conjunction with article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC). Just recently, the Court of Justice of the European Union (CJEU) resolved that this also 'covers the provision of online information services for which the service provider is remunerated, not by the recipient, but by income generated by advertisements posted on a website'.[101]

In addition, the Consumer Rights Directive requires the consumer 'pays or undertakes to pay the price' in exchange for a service (cf 2(6) of the Consumer Rights Directive). The literature discusses whether in some circumstances individual consumers' personal data could be regarded as a price in an exchange relationship with the service provider.[102] However, for consumer-facing cloud services this would aggravate the lack of control and privacy because it implies that the commodification of individual users' personal records is acknowledged barter in exchange for a free service. What could perhaps be argued in the case of freemium consumer-facing cloud services is that only the basic offer is free of charge, but a prospective payment is to be expected if consumers' upgrade to a paid for service. Thus, quite some legal uncertainty persists over the applicability of EU consumer protection law to free consumer-facing cloud offerings.

Where standard terms of service contain a provision on the choice of law that direct judicial review to the laws of a specific jurisdiction, this is likely not to withstand

99 cf Cunningham and Reed (n 6) 334.

100 H Schulte-Nolke, C Twigg-Flesner and M Eberts, *Consumer Law Compendium* (2008) 713 <http://www.eu-consumer-law.org/study_en.cfm> accessed 10 June 2015.

101 Case C–291/13 *Sotiris Papasavvas v O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis* (CJEU, 11 September 2014) para 30; NB: in CJEU jurisprudence the lack of a payment does not disqualify services that from protection under the freedom to provide services according to art 57 Treaty on the Functioning of the European Union (TFEU), cf Case C–155/73 *Giuseppe Sacchi* [1974] ECR 409 (CJEU, 30 April 1974); Case C–352/85 *Bond van Adverteerders v the Netherlands* [1998] ECR 2085 (CJEU, 26 April 1988).

102 In favour in the context of social network services Wauters, Lievens and Valcke (n 59) 10; differentiating between free online services Helberger and others (n 9) 165.

EU consumer protection law. Article 6(2) of the Unfair Terms Directive guarantees that the consumer is protected in spite of a choice of law clause in a contract if she is residing in a Member State.[103] For example, a French judgment against a social networking site invalidated the choice of law provision directing users to the jurisdiction of Delaware, a state in the USA, because the user did not enter into this term with full knowledge.[104] By now, many cloud service providers' standard terms of service direct EU individual consumers to their national jurisdictions.

### *Transparency and information requirements*

EU consumer protection law renders an important contribution to the transparency and completeness of information a (prospective) individual cloud consumer receives. Article 5 of the Unfair Commercial Practices Directive requires written terms to be drafted in plain, intelligible language. Article 6 of the Consumer Rights Directive, which applies to any contract concluded between a trader and a consumer, stipulates compulsory information requirements for distance and off-premises contracts. In addition, Article 5 of the E-Commerce Directive obliges the provider information society services to provide a set of general information to the recipients and under its article 10 clear information about the transaction before an order is placed by the recipient of the service.

Many consumer-facing cloud services will also meet the definition of digital content contracts in article 2(11) for which case the Consumer Rights Directive prescribes customized information duties, among others about the functionality and the relevant interoperability of digital content.[105] Information about the functionality should explain consumers how digital content can be used and whether it involves the tracking of consumer behaviour (article 5(1)(g) of the Consumer Rights Directive). Relevant interoperability information requires the provider to set out the hardware and software requirements with which the digital content is compatible (article 5(1)(h) of the Consumer Rights Directive).

### *Unfair commercial practices*

The standard terms of service of consumer cloud offerings, which are unilaterally stipulated by the service provider, can be scrutinized in the light of the Unfair Terms Directive. Standard terms of service are deemed unfair if they contain a term listed in the Annex to the Directive or fail to meet the general clause of article 3(1) of this Directive. It is the legal consequence of an unfair term that it is not binding on the consumer but the remainder of the contract continues to bind the parties if possible (article 6(1) of the Unfair Terms Directive).

103 cf European international civil law provisions applicable to consumers under Brussels I and Rome I regulations.

104 Case RG 12/1373 *Sebastian R v Facebook* (Court of Appeal (Pau), 23 March 2012), <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3382> accessed 10 June 2015; discussed in Cunningham and Reed (n 6) 353.

105 cf Recital 19 of the Consumer Rights Directive. Note in addition the modified right of withdrawal for consumers of digital content services (art 16(mm) of the Consumer Rights Directive) and payments when it is exercised (art 14(4)(b) of the Consumer Rights Directive).

Certain common provisions on termination and unilateral changes of the standard terms of service or the service characteristics are actually listed in the Annex of the Directive as *prima facie* unfair terms (cf lit (g), (j) and (k) of the Annex).[106] For example, the Norwegian Consumer Council submitted a complaint against a popular cloud service provider whose terms allegedly infringe the Unfair Terms Directive and the Norwegian Marketing Act.[107] The contested term concerns the service provider's unilateral right to change the agreement at any time, at its own discretion and without giving users' notice.

Under the general clause a term is regarded unfair if, 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer'.[108] Whether standard terms of service of consumer-facing cloud services would carry such a significant imbalance is yet unresolved. While it is under article 4 possible to take into account the nature of the services for which the contract was concluded, it is not possible to incorporate additional considerations, such as the transformation of personal record-keeping practices and the loss of control on part of individual cloud consumers in assessing the unfairness of a term. Moreover, when cloud services are provided to individual consumers free of charge, an appraisal of the standard terms and conditions may simply not justify higher expectations with a view to the obligations of the service provider.

It is widely acknowledged that the present, highly fragmented legal framework is neither particularly relevant for cloud services nor adequate to protect consumers' personal records in the cloud against risks and disenfranchising commercial practices of the service provider. Alone, data protection law where it applies would require cloud service providers to obtain individual consumers' unambiguous consent for processing personal records for secondary purposes. Some relief can be expected from the EU data protection reform which was clearly drafted having cloud services in mind. In order to come to terms with the fragmented protection under different legal regimes, DLA Piper in their comparative study on cloud computing contracts concludes:

> [I]t is highly recommended from a general contracting perspective, in case contracting parties wish to avoid having discussions on rights on content, [to] include provisions on confidential information in the cloud contract.

## EU CLOUD COMPUTING POLICY

The European Commission's cloud computing strategy of 2012 is cognizant of the shortcomings of today's legal framework pertaining to cloud computing offerings to individual consumers.[109] Herein the Commission proposes as one key action the

106 DLA Piper UK LLP (n 4) 52.

107 The Norwegian Consumer Council, 'Complaint Regarding Apple iCloud's Terms and Conditions' (2014) http://www.forbrukerradet.no/_attachment/1175090/binary/29927 accessed 10 June 2015; Crisp.

108 Art 3(1) of the Unfair Commercial Practices Directive.

109 European Commission.

development of European model contract terms and conditions in order to create transparent and fair cloud services contracts. The Commission took the stance that such model contract terms will accelerate the take-up of cloud computing by increasing the trust of prospective consumers. The model contract terms intended to cover a range of pertinent issues for cloud consumers that are presently unregulated, notably:

- data preservation after termination of the contract,
- data disclosure and integrity,
- data location and transfer,
- ownership of the data [*sic*],
- direct and indirect liability change of service by cloud providers and subcontracting.[110]

While the conclusion of this activity was foreseen for 2013 this is yet to happen. There is actually no commitment as to when the 'safe and fair' model contract terms and conditions would be presented.

## CONCLUSIONS

This article focuses on the legal protection of unpublicized personal records that individual consumers place into the custody of public cloud services. It aims to assess the transformational impact of cloud sourcing on the legal protection of individual consumers' information. Against the backdrop of the transformation of personal record-keeping practices, I argue that the disruption of physical control and cloud services' commercial propositions produce a backslide for individual positions of rights. Reed's conclusion that the composite effect of sectoral laws confers 'a level of control over [ . . . ] information which is very similar to owning physical property' does not accurately depict the situation of individual cloud consumers.

Provided that any legal assessment would be highly determined by the case-specific circumstances, sectoral laws applicable to the situation of cloud services seem to produce disparate levels of protection and even gaps where no protection is afforded to personal records. As for the contractual arrangement, the standard terms of service tend to be biased in favour of the service provider and fall short in achieving a fair balance with individual consumers' interests in security and control. While providing for needed transparency and information duties, it is not within the purview of EU consumer protection law to correct a factual development that has led to personal records being intermediated by providers of cloud services. Only from a contract law perspective certain unfair terms would be rectified where they create a significant unbalance in the parties' rights and obligations under the contract. EU data protection law offers some protections, however insufficient, to guarantee individuals' privacy and control over personal records residing in the cloud.

The intermediation of personal affairs is not a new phenomenon. Pre-dating cloud computing, the more traditional information intermediaries, such as mail and telecommunications services, take a similar effect and they are regulated. The secrecy of

110 As listed on the website of the European Commission <http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy> accessed 20 June 2015.

correspondence and communications is a legal institute throughout Europe, in a range of countries of constitutional value, which protects individuals' communication also vis-à-vis the service provider.[111] What is perhaps a new issue with cloud computing is that there is no comparable legal paradigm that protects individuals' personal records when at rest under the control of a third party.

Not only that legal uncertainties surrounding these issues can undermine the confidence of users and service providers, but consequently, the widespread adoption of these services and the emergence of new business models may also be delayed as a result of an inadequate governance framework. But the lacking understanding of the individual dimensions of the ongoing transformation and its socio-economic and societal impact could be misjudged diverting policy makers and stakeholders attention to issues of privacy and security while there is decisively more at stake.

Future research should be directed at individual cloud customers' fundamental rights at stake and whether data protection law is the adequate legal instrument for cloud-sourced personal records of individual consumers. What is perhaps needed is a new legal paradigm that better corresponds with a virtual private sphere and allocates essential control to individual consumers. As Schneier writes in his latest book *Data and Goliath*:[112]

> We need information fiduciaries. The idea is that they would become a class of organization that holds personal data, subject to special legal restrictions and protections. (. . .) Perhaps some types of business would be automatically classified as fiduciaries simply because of the large amount of personal information the naturally collect. (. . .) Fiduciary regulation would give people confidence that their information wasn't being handed to the government, sold to third parties or otherwise used against them.

While this argument emanated from several US scholars it is not less relevant in the European context this article concludes.

111 Paul de Hert, Bert-Jaap Koops and Ronald Leenes, 'Constitutional Rights and New Technologies: A Comparative Perspective' in Caroline Pauwels and others (eds), *Rethinking European Media and Communications Policy* (VUB Press 2009) 319–50, 336f. It did, however, not prevent the automated scanning of email content for keywords in order to display targeted advertisement alongside the content of an email message.

112 Bruce Schneier, *Data and Goliath, the Hidden Battles to Collect Your Data and Control Your World* (WW Norton & Company 2015) 205. cf. Jack Balkin, 'Information Fiduciaries in the Digital Age' (Wednesday, March 05, 2014, 2014) <http://balkin.blogspot.co.uk/2014/03/information-fiduciaries-in-digital-age.html> accessed 10 June 2015; Jonathan Zittrain, 'Engineering an Election' (2014) 127 Harvard Law Review Forum 335-341.