A right too far? Requiring cloud service providers to deliver adequate data security to consumers

Kevin McGillivray*

ABSTRACT

The European consumer has substantial rights when contracting for goods or services online. Nevertheless, unlike European data protection law, specific requirements for adequate data security practices are largely absent from European legislation governing Business-to-Consumer (B2C) transactions. The following article evaluates the application of current EU consumer protection requirements and appraises the extent to which they oblige service providers to include data security or information regarding data security practices in contract terms. In addition to considering the core European consumer protection instruments currently in place, the article evaluates proposed legislation for digital goods and assesses its potential application to contract terms commonly offered by cloud service providers (CSPs). Furthermore, the article provides some comparative analysis of data security requirements from the USA.

KEYWORDS: consumer protection, contracts, cloud computing, data security, digital content, unfair contract terms

INTRODUCTION

The following article evaluates central aspects of EU consumer protection legislation and their application to data security requirements. Although EU consumer protections are substantial, a specific requirement for adequate data security practices—either informational or actual—is currently absent in legislation governing Business-to-Consumer (B2C) transactions. The article considers consumer protection compliance requirements as they are now, evaluates the elements of a proposed directive and appraises whether further steps should be taken to address data security in consumer contracts or services. In other words, ought EU consumer protection regulations oblige providers to include information on their data security practices or provide a minimum level of security? While maintaining a data security focus, the article further evaluates the impact of contract terms allowing providers to amend...
contract terms or service provisions unilaterally. The article makes some comparison with data security requirements and consumer protection in the USA by examining a recent case.

When purchasing digital services, consumers are often contracting for a ‘product’ containing attributes of both goods and services without falling firmly under either category. The seller provides a method of delivery, addresses compatibility and even functionality with varying degrees of opaqueness. In comparison to the experience of a consumer in the offline world, the purchaser of digital services or content faces new challenges. For example, if a consumer needs storage for paper documents, they can more readily assess whether the physical unit they plan on renting meets their needs. The consumer can visit the site of the property owner to evaluate if it is of adequate size and safe for the type of goods they plan on storing. If the roof of the building has holes or the unit is missing a door, the consumer can simply leave, as they will have observed the inadequacy of the space. Although not all information is available, such as the financial stability of the property owner or whether other renters have dangerous goods stored in their connected individual units, the consumer does not have to be an expert on building design to understand what the seller is offering and the risks they are taking by accepting the offer. In most jurisdictions, the consumer also has some assurance that certain building safety codes are applicable to the facility and the consumer can generally obtain insurance to cover losses not insured by the storage provider.

If that same consumer is interested in renting storage for their digital belongings on a cloud computing service, conceptualizing understanding the ‘space’ is more difficult. In the cloud scenario, it is unlikely that the consumer can drop by the cloud service provider (CSP)’s office and ‘kick the tires’ to see if everything is in order. While the consumer may be periodically provided with a copy of a third-party audit, the report might not contain information that specifically addresses the consumer’s needs. Even finding out where a service is located or a contact point if things go wrong can be challenging. Other questions regarding availability, functionality, and security are often left out. For example, does the content contain Digital Rights Management (DRMs) technologies restricting or limiting the consumer’s use of the content? Will the digital content be accessible or usable on competing platforms? Do

---

2 The contract terms included in cloud computing agreements are neither defined nor used consistently in either contracts or legal literature. As noted by one author, ‘[t]he nomenclature is somewhat bewildering, especially as it is often used imprecisely and interchangeably.’ Lee A Bygrave, *Internet Governance by Contract* (OUP 2015) 38. For the purposes of this article, ‘terms’ describes the many parts of a cloud computing agreement.

3 Clarice Marinho Martins de Castro, Chris Reed and Ruy JGB de Queiroz, ‘Digital Content and Cloud-based Contracts in Brazil and the European Union’ (2016) 24 International Journal of Law and Information Technology 99–118, 105. For a discussion based on categorization of cloud computing under the national laws of EU Member States, see European Commission, ‘Comparative Study on Cloud Computing Contracts’ (2015) (‘EC Contract Study’) <http://ec.europa.eu/justice/contract/cloud-computing/studies-data/index_en.htm> accessed 26 June 2016.

4 Peter Mell and Tim Grance, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (US National Institute of Standards and Technology 2011) 2–3. Providing a widely used definition of cloud computing.
the licensing conditions limit certain types of use, claim rights over the consumer’s content, or contain jurisdictional restrictions?\(^5\)

At the same time, there are many other issues the consumer ought to consider, including the location of the infrastructure, warranties provided, rights retained by the consumer over their data, and whether their data’s storage format is common or can be transferred to formats used by other providers. Closely related to these fundamental aspects, many cloud offerings provide little information regarding their data security practices. When describing data security, many of the contract terms offered by CSPs provide little, or very generic, information in this regard, using phrases such as ‘industry standard’ or ‘commercially reasonable’.\(^6\) Furthermore, although data security is addressed in ‘data protection’ legislation in the EU, there is little focus on data security under current EU ‘consumer protection’ legislation.\(^7\) Although data protection legislation will apply to many consumer transactions, it will not apply in all cases.\(^8\)

Irrespective of the information provided in a contract or privacy policy, the presence of adequate data security is important because in areas where it is lax, the consequences to consumers in the form of identity theft, swindle and lost data are often high. Moreover, the consequences of consumer unwillingness to make digital purchases are also costly for the Digital Single Market (DSM).\(^9\) In its DSM strategy, the European Commission specifically noted that as a result of security and related concerns, consumers still do not feel confident enough to adopt cloud services.\(^10\)

The analysis of whether EU consumer protection contains or ought to contain consumer protection against inadequate data security practices takes the following path. First, what do current consumer protection regulations require regarding data security practices by CSPs or other digital content providers? Secondly, are the proposed directives—to the extent that they consider the problem of data security—sufficient or likely to provide consumers with effective protection? Thirdly, how might the proposed legislation impact contract terms commonly expressed in cloud computing agreements?

This article is divided into four main sections. Section 1 provides the introduction. Section 2 analyses aspects of the current EU framework ‘as it is’. Section 3 considers

---

5 Marco BM Loos and others, ‘Analysis of the Applicable Legal Frameworks and Suggestions for the Contours of a Model System of Consumer Protection in Relation to Digital Content Contracts’ (2011) 46 <http://ec.europa.eu/justice/consumer-marketing/files/legal_report_final_30_august_2011.pdf> accessed 26 June 2016.
6 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’ (2015) Queen Mary School of Law Legal Studies Research Paper No 209/2015, 51–52 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2646447> accessed 26 June 2016.
7 For a description of the role of data security in the European and international data protection context, see Lee Bygrave, Data Privacy Law: An International Perspective (OUP 2014) 164–65.
8 Elaborated in s 3.1.
9 European Commission, ‘A Digital Single Market Strategy for Europe’ Brussels, 6 May 2015 COM (2015) 192 final (hereinafter ‘Digital Single Market Strategy’ or ‘DSM’) 4 <http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf> accessed 26 June 2016. See proposed DCD, Recital 4.
10 ibid 14.
the current role of data security in consumer protection and evaluates the proposed legislation. Section 4 provides the conclusion.

The ‘law between parties’ and contracts for digital content or services

As a starting point, many of the rules governing the purchase of digital services are derived from the contract between the parties. The argument can be made that if users want increased data security for cloud computing services, they ought to bargain for more security during the contracting process. However, that logic rapidly parts ways with the current reality regarding the ability of consumers to negotiate when contracting for digital content or services. For most consumers using cloud computing or other digital services, the suggestion that they have sufficient bargaining power to negotiate and obtain changes to standard term agreements is unrealistic. In principle, consumers can refrain from using a service if the terms are unacceptable and the CSP refuses to come to the bargaining table. However, doing so may limit consumer access to modern necessities, such as communications services including email, Internet access and even services that have traditionally been offline, such as banking. Refusing the terms offered by a CSP may even limit access to software or popular programs that are increasingly being delivered on cloud-based platforms. Discussing online contracting, one author provided the following observation:

There is perhaps no area of law with a more obvious disconnect between fundamental premises and modern reality than contracts. One of the most basic ideas in contract law is the notion of freedom of contract—parties may, with minimal limitations, enter into contracts with one another on such terms as they see fit. Of course the corollary to this freedom is that if one party does not like the deal being offered, that party is free to walk away and look for a better set of terms elsewhere.

Although consumers may have the freedom to walk away from the terms offered by a CSP, finding better or adequate terms elsewhere is an unlikely proposition. A consumer will most likely find very similar terms, equally one-sided, from competing providers. At the same time, the number of agreements consumers enter into continues to rise, while the terms themselves remain in conflict with many core privacy

11 Emily M Weitzenböck, A Legal Framework for Emerging Business Models: Dynamic Networks As Collaborative Contracts (Edward Elgar Publishing 2012) 150.
12 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 International Journal of Law and Information Technology 254–94 <http://ijlit.oxfordjournals.org/cgi/doi/10.1093/ijlit/eau002> accessed 26 June 2016.
13 In Norway, for example, several banks operate entirely online without any physical locations in the country <https://skandiabanken.no/> accessed 26 June 2016.
14 Certain Software as a Service (SaaS) providers (eg Salesforce and Amazon Web Services) focus increasingly on a cloud-based rather than traditional on-premise software licensing models.
15 John A Barrett Jr, ‘It’s Time for a Good Hard Look in the Mirror: The Corporate Law Example’ (2012) 17 Fordham Journal of Corporate & Financial Law 943, 949.
and consumer protection principles.\textsuperscript{16} Although the focus of this article is on consumers, asymmetrical contracting relationships—and their resulting consequences—are not necessarily restricted to consumers. The situation also applies to small- and medium-sized enterprises (SMEs) and even municipalities contracting with CSPs.\textsuperscript{17}

Adding a further layer of abstraction for consumers is that what is allowed or can be enforced in a standard agreement varies among jurisdictions. In particular, this gap exists between the EU and the USA. In the EU, ‘regulators have been expanding their oversight . . . at precisely the time that USA contract law has turned away from public regulatory models’.\textsuperscript{18} In the EU Member States, the rights of consumers are prioritized and a more ‘protective’ or ‘paternal’ approach is taken.\textsuperscript{19} Although the parties are free to contract, EU consumer protection legislation puts limits on that freedom.\textsuperscript{20} In other words, the EU approach does not allow consumers to waive some rights regardless of the terms consumers accept in the contracting process.\textsuperscript{21} In the USA, consumer protection legislation is generally much weaker and many of the rights granted to consumers can be bargained away in the terms of the contract.\textsuperscript{22} Unlike the EU, the USA continues to apply the principle of caveat emptor to B2C transactions in addition to agreements entered on a Business-to-Business (B2B) basis.\textsuperscript{23}

The reality of the situation is that consumers, even if protected in their home jurisdictions, may face uneven and somewhat unpredictable representation of their local consumer rights in contract terms offered by CSPs. In other words, although EU legislation provides European consumers with certain rights, exercising or realizing those rights can be difficult, particularly in the cloud computing context.\textsuperscript{24} In the European Commission strategy, the need for ‘safe and fair’ contract terms in cloud computing was considered particularity acute in the consumer context.\textsuperscript{25} An expert

\begin{itemize}
\item \textsuperscript{16} K Stylianou, J Venturini and N Zingales, ‘Protecting User Privacy in the Cloud: An Analysis of Terms of Service’ (2015) 6(3) European Journal of Law and Technology 3. Finding a ‘suboptimal level of protection’ of consumer protection in cloud computing contracts.
\item \textsuperscript{17} Alberto G Araiza, ‘Electronic Discovery in the Cloud’ (2011) 10 Duke Law and Technology Review 16, para 36 <http://dltr.law.duke.edu/2011/09/20/electronic-discovery-in-the-cloud/> accessed 26 June 2016. Alan Cunningham and Chris Reed, ‘Consumer Protection in Cloud Environments’ in Christopher J Millard (ed), Cloud Computing Law (OUP 2013) 331–61, 337.
\item \textsuperscript{18} ibid 3.
\item \textsuperscript{19} Andrej Savin and Jan Trzaskowski, Research Handbook on EU Internet Law (Edward Elgar Publishing Ltd 2014) 255.
\item \textsuperscript{20} Michael L Rustad and Maria Vittoria Onufrio, ‘Reconceptualizing Consumer Terms of Use for a Globalized Knowledge Economy’ (2012) 14 University of Pennsylvania Journal of Business Law 1085, 1116 <https://www.law.upenn.edu/journals/jbl/articles/volume14/issue4/RustadOnufrio14U.Pa.J.Bus.L.1085%282012%29.pdf> accessed 26 June 2016.
\item \textsuperscript{21} Savin and Trzaskowski (n 19) 255.
\item \textsuperscript{22} Dan Svantesson and Roger Clarke, ‘A Best Practice Model for E-consumer Protection’ (2010) 26 Computer Law & Security Review, 3.
\item \textsuperscript{23} Rustad and Onufrio (n 20) 1132.
\item \textsuperscript{24} European Commission (EC), ‘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) (‘EC Unleashing’) 12 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0529&from=EN> accessed 26 June 2016.
\item \textsuperscript{25} ibid.
\end{itemize}
group on cloud computing contracts was appointed by the European Commission to explore and potentially draft ‘safe and fair’ model contract terms that could be applied to SMEs and consumers acquiring cloud services, focusing on areas such as data location, liability, data preservation and subcontracting. However, model terms have not been completed and the creation of any such terms by the current expert group seems unlikely.

The European Commission is not alone in singling out the contracting practices of CSPs as problematic or inconsistent with the rights of consumers. In addition to Data Protection Authorities (DPAs), consumer protection authorities, such as the Office of the Civil Ombudsman in Norway, have taken issue with contact terms and conditions being offered as illegal pursuant to national laws. In Norway, the charge has been made that many of the terms provided in Apple’s iCloud service—among those of other CSPs—are illegal. The terms violate both EU and Norwegian law in many areas, including warranties/liability, limited privacy protections, and variation or amendment of contract terms without acquiring new consent.

Although the USA and the EU may be ‘oceans apart’ on consumer protection law, US regulators have also been critical of contracting practices by CSPs and other digital content providers. The USA focus has been primarily on misleading consumers coupled with an increased focus on data security. Notably, the US consumer protection authority, the Federal Trade Commission (FTC), has fined individual providers for unfair trade practices for overstating the levels of security they provide in contract terms or privacy polices (eg encryption levels and application in their services). How this position might apply to CSPs, and whether it should be adopted in the EU, is explored in Section 3.

THE EU FRAMEWORK FOR CONSUMER PROTECTION ‘AS IT IS’

In applying the EU Framework, the first question is to whom do the protections apply? Although there is no uniform definition of ‘consumer’, European legislation generally labels natural persons acting outside of their trade or profession as such. In order for EU consumer protection legislation to apply, the party asserting the protections must be a consumer. Determining when a party is acting as a consumer, or as a hybrid consumer, versus as a professional party is becoming more difficult in the

26 European Commission (EC), ‘Expert Group on Cloud Computing Contracts’ <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm> accessed 26 June 2016.
27 Ruxandra Gabriela, ADAM Policy Officer European Commission, ‘Email to Author Regarding the Outcome of the Expert Group on Cloud Computing Contracts’ (17 February 2016).
28 Norwegian Consumer Council, ‘Apple iCloud Violates Norwegian and European Law’ (13 May 2015) <http://www.forbrukerradet.no/pressemelding/apple-icloud-violates-norwegian-and-european-law/> accessed 26 June 2016.
29 ibid. For an updated study focusing on consumer applications, see Finn Lützow-Holm Myrstad and others, ‘APPFAIL: Threats to Consumers in Mobile Apps’ (March 2016) <http://fbrno.climg.no/wp-content/uploads/2016/03/Appfail-Report-2016.pdf> accessed 26 June 2016.
30 Sebastian Zimmeck, ‘The Information Privacy Law of Web Applications and Cloud Computing’ (2012) 29 Santa Clara High Technology Law Journal 34, fn 63.
31 For instance, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights OJ L 304/2011 (‘CRD’) art 2(1) (emphasis added).
context of services like cloud computing.\textsuperscript{32} In considering questions of applicability, the dispositive factor in determining whether a party is a consumer or a professional is their status at the time the contract was entered into.\textsuperscript{33} In other words, contracts entered into by consumers will generally receive consumer law protections even if their status changes later.

If the party entering into an agreement is a consumer, the EU provides an inclusive and multifaceted system of consumer protection and guarantees. On that basis, consumers ought to be able to extend this expectation—that their rights are protected—to purchases made in the digital marketplace on a national and even a global level.\textsuperscript{34} The application of EU protections covers the entire ‘lifecycle’ of a consumer contract, from the advertisement of a service to the contract ‘offer’ and ‘formation’ of a contract, through to procedural and substantive issues regarding the content of terms, including terms for the ‘termination’ of the contract, and finally setting the rules governing the ‘how’ and ‘where’ disputes will be adjudicated if the need arises.\textsuperscript{35} This ‘cradle-to-the-grave’ coverage is achieved by offering consumers remedies at several stages or levels of the contracting process in addition to making certain unfair terms unenforceable. By creating a ‘floor’, or minimum standard, that allows consumers to disaffirm contracts based on subjective dissatisfaction or ‘buyer’s remorse’, the European consumer has substantial rights when they enter into contracts online.\textsuperscript{36}

These rights are further expressed in a series of EU directives and regulations that are intended to protect consumers and are applicable to consumers using cloud services, the most central of which are the following: the Unfair Terms Directive (UTD); the Unfair Commercial Practices Directive; and the Consumer Rights Directive (CRD), among others.\textsuperscript{37} In addition to consumer-specific legislation, Brussels I (jurisdiction) and Rome I (law applicable in contractual matters) also have consumer-specific provisions—in addition to broader regulatory application.\textsuperscript{38} Many of the contract terms offered by USA-based CSPs are at odds with the mandatory European consumer protection legislation described above.\textsuperscript{39} This article focuses primarily on the UTD and the CRD; however, as outlined above, others are also potentially applicable.

\textsuperscript{32} Cunningham and Reed (n 17) 331. Discussing the difficulty SMEs have in negotiating such terms and opining that consumers have even less ability to obtain negotiated or customized agreements.

\textsuperscript{33} ibid 336.

\textsuperscript{34} Beatriz Añoveros Terradas, ‘Consumer Collective Redress under the Brussels I Regulation Recast in the Light of the Commission’s Common Principles’ (2015) 11(1) Journal of Private International Law 143–62, 149. Evaluating art 18(1) of the Brussels I Regulation Recast.

\textsuperscript{35} Regulation (EC) No 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I). See Council Regulation (EC) No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) (Brussels I).

\textsuperscript{36} See Rustad and Onufrio (n 20).

\textsuperscript{37} Council Directive (EC) 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 1993 29–34 (‘UTD’). Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair B2C commercial practices in the internal market, OJ L 149/2005, CRD. The 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 (ECD) also has application.

\textsuperscript{38} See Brussels I and Rome I (n 35).

\textsuperscript{39} Rustad and Onufrio (n 20) 1116. Maintaining that many of the one-sided USA-style contracts are simply not enforceable in Europe.
The UTD is designed to mitigate the effects of the significant imbalances in contracts made between consumers and professional parties, such as CSPs. An important objective of the UTD is to help consumers choose products from Member States without fear by reducing or eliminating ‘misleading’ or ‘unfair’ practices. Simply stated, where unfair terms are provided, the UTD makes those terms unenforceable against consumers.

The UTD’s substantial protections are intended to increase consumer confidence, consumer choice, and reduce confusion or hesitation in engaging in cross-border transactions. For example, the UTD provides that “[i]n the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language.” Where there is doubt about the meaning of a term, the ‘interpretation most favourable to the consumer shall prevail.’ The UTD applies to contracts that are not individually negotiated. In areas such as cloud computing, the UTD has wide application as few cloud contracts entered into by consumers take place on a negotiated basis. Contracts that are ‘drafted in advance’ and do not provide any opportunity for consumer input or those presented as ‘pre-formulated standard contracts’ will be regarded as not being individually negotiated for the purposes of the directive. Therefore, the take-it-or-leave-it contracts commonly offered for cloud computing services meet this designation.

In addition to requiring ‘plain’ or ‘intelligible’ contract terms, the UTD provides guidance on the types of contract terms that are illegal or cannot be enforced against consumers while also codifying the concept of ‘good faith’ into EU contracting law. More concretely, a non-negotiated contract term will be regarded as 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.’ Although the conjunctive drafting of the test to be applied by courts requires that two primary elements be met, the key or main aspect a court considers is whether the contract is ‘fair’. As stated concisely by one author, ‘the prevailing—and more correct interpretation of the UTD—is that any contractual term in a consumer contract causing a significant imbalance is by definition contrary to the principle of good faith.’ However, this fairness test, and what is considered to be unfair regarding consumers, varies among Member States.

As the UTD is not ‘fully harmonized’, it sets the ‘floor’ and not the ‘ceiling’ for consumer rights. The UTD Annex essentially takes many of the aspects or contents...
of existing standard terms and highlights the most unfair elements. For example, contract terms that are to the seller’s advantage exclude all liability stemming from injury, excuse or limit a seller’s liability for non-performance under the contract, provide illusory promises by the seller, and terms requiring excessive payments in the form of damages for cancellation.\textsuperscript{51} Other terms in the Annex relate to requiring that a consumer be held to unreasonable timelines for cancellation of an agreement or allowing a seller to cancel a contract unilaterally without adequate grounds.\textsuperscript{52}

Although B2B terms requiring that a dispute be resolved in the CSP’s home jurisdiction may be valid, limits on a consumer’s right to access their local courts will often be adjudicated as unfair and thus invalid. A consequence of having many USA-based CSPs is that they do not always adjust their terms for European consumers.\textsuperscript{53} Hence, many contract terms offered by USA-based CSPs violate EU law.\textsuperscript{54} Although the USA does have a legal tradition of protecting consumers from unfair trade practices by voiding ‘unconscionable’ contract terms, the approach and protections it offers are limited when compared to the legal setting in the EU.\textsuperscript{55} For a consumer to escape enforcement of a term, they must generally show that the terms of the agreement are ‘unconscionable’ and in some way ‘shock the conscience’, are ‘surprising or unexpected’, or for public policy reasons should be void. This is an exacting standard. The result is that many of the ‘prohibited terms’ in the UTD are prevalent in cloud computing agreements because they are designed for a US market where they do not violate legal requirements.

As a final note, one of the strengths of the UTD—at least from the consumer standpoint—is that it is drafted broadly. Although the UTD provides clear examples of unfair terms in its Annex, many more that are not identified directly would nevertheless be invalidated based on its broad scope. In that sense, the UTD plays an overlapping role with other instruments and provides an extra layer of protection for consumers.\textsuperscript{56} However, the Annex was drafted over 20 years ago, and although many of the provisions are relevant to digital content and cloud computing, they are not specific to those environments.

CRD

In 2014, the CRD came into force replacing existing directives regulating distance contracts.\textsuperscript{57} The updated CRD makes clear certain obligations between buyers and sellers, with a particular focus on electronic means of entering into agreements covering specific aspects of the digital environment. The directive does not allow Member

\begin{itemize}
\item \textsuperscript{51} UTD Annex (a-e) paraphrasing.
\item \textsuperscript{52} UTD Annex (g) paraphrasing.
\item \textsuperscript{53} Simon Bradshaw, Christopher Millard and Ian Walden, ‘Standard Contracts for Cloud Services’ in Millard (n 17) 39–72, 68.
\item \textsuperscript{54} Rustad and Onufrio (n 20) 1135.
\item \textsuperscript{55} ibid 1136. Comparing the US unconscionability doctrine to the European approach finding a much lower limit for intervention by European courts.
\item \textsuperscript{56} Wauters, Lievens and Valcke (n 12) 23. Citing UTD Annex q.
\item \textsuperscript{57} European Commission (EC), DG Justice, ‘Justice Guidance Document Concerning Directive 2011/83/ EU of the European Parliament and of the Council of 25 October 2011’ (2014) <http://ec.europa.eu/justice/consumer-marketing/files/crd_guidance_en.pdf> accessed 26 June 2016.
\end{itemize}
States to diverge from the mandatory terms of the agreement and is imposed as a full harmonization directive.\textsuperscript{58}

At its core, the CRD is intended to increase consumer protection. The CRD provides bright-line rules for distance and off-premise contracts, affords a uniform period for consumers to withdraw from agreements, and requires stricter pre-contractual and other informational requirements. Moreover, the CRD has broad application and applies to ‘any contract concluded between a trader and a consumer,’ with the exception of contracts in certain categories.\textsuperscript{59} However, whether the CRD is also applicable to ‘free’ services has been a point of discussion. For example, in Article 2 of the CRD, the following text is provided:

\textbf{(5) ‘sales contract’ means any contract under which the trader transfers or undertakes to transfer the ownership of goods to the consumer and the consumer pays or undertakes to pay the price . . . [.]},

\textbf{(6) ‘service contract’ means any contract other than a sales contract under which the trader supplies or undertakes to supply a service to the consumer and the consumer pays or undertakes to pay the price thereof. (emphasis added)}

Although ‘paying the price’ also includes the use of gift cards or reward points, at first blush it does not appear to apply to services provided for ‘free’. Consumers, unlike governments or businesses, often obtain cloud services on a data-for-use rather than a payment-for-use basis.\textsuperscript{60} However, it appears that there are exceptions to this requirement. For instance, at Article 2 (11), the CRD applies to digital content, meaning ‘data which are produced and supplied in digital form’ are exempted from the payment requirement. Therefore, a consumer downloading a free application or song would apparently be protected under the CRD and the rights provided in the CRD would apply to the digital purchase.

Nevertheless, the question remains, how should services where a consumer ‘pays with privacy’ for use of the service, but where no digital good is obtained, be treated under the directive? It has been well documented that many services, including cloud offerings, are supported by the information obtained from users for advertising or other purposes.\textsuperscript{61} Trading personal information used to create advertising or potentially to convert the consumer into a paying customer is exchanged for ‘free’ use of the service. How then, should a customer using a free Infrastructure as a Service (IaaS) application be treated under the directive? Is this equivalent to downloading a song or installing an application? In any event, even if the CRD does not apply, or

\textsuperscript{58} CRD art 4.

\textsuperscript{59} CRD art 3(3). See Recitals 26–31 for scope of exclusions.

\textsuperscript{60} National Institute of Standards and Technology (NIST) has categorized classes of ‘public clouds’ based on whether the service is paid for by traditional remuneration (payment-for-use) or supported by advertising (data-for-use). Wayne Jansen and Timothy Grance, \textit{Guidelines on Security and Privacy in Public Cloud Computing}, Special Publication 800-144 (NIST 2011) 6 <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf> accessed 26 June 2016. For examples of ‘data-for-use,’ see Chris Jay Hoofnagle and Jan Whittington, ‘Free: Accounting for the Costs of the Internet’s Most Popular Price’ (2014) 61 University of California Los Angeles Law Review 606, 626–28.

\textsuperscript{61} Wauters, Lievens and Valcke (n 12) 10.
provides a lower standard of protection for free services, it does not seem that cloud computing services supported by consumer data as a form of remuneration are excluded from CRD application. After all, the consumer is paying for the service, albeit with privacy rather than conventional currency.

The CRD requires that information regarding the duration of the contract, renewal requirements (ie automatic extensions of the agreement), and the consumer’s obligations under the agreement are provided. Cloud contracts may not have a set duration and are often provided on monthly or yearly subscription basis. As potential long-term contracts, the CRD requires that the CSP provides the consumer with information regarding conditions for terminating the contract. The CRD also requires that consumers be provided with certain information regarding their right to withdraw from a service. These include application of the right, procedures for exercising the right, the consumer’s obligations for the costs of returning goods, and the obligation of the consumer to bear the trader’s reasonable costs.

**General information that CSPs and other sellers must provide**

For consumers, simply contacting a digital services provider can pose a challenge. To overcome this hurdle, several of the consumer protection instruments require that the seller provides at least a basic level of information regarding the transaction. This requirement starts with a name, address and other contact details. In addition to information about the seller, consumer protection rules require that the seller provides information regarding technical requirements in addition to price. For instance, the CRD requires clear information on the total price of the service including all taxes and ‘hidden’ charges.

Information regarding both the functionality and interoperability of the product being offered is also required. Specifically, the seller must present ‘any relevant interoperability of digital content with hardware and software that the trader is aware

---

62 For exemptions (eg healthcare services), see CRD arts 8(2), 19 and 22.
63 CRD arts 5(1)(f), 6(1)(o) and (6)(1)(p).
64 CRD art 5(1)(f). The CRD also provides consumers ‘…14 days to withdraw from a distance or off-premises contract, without giving any reason…’ CRD art 9(1).
65 CRD art 6(1)(h-k). See CRD art 9.
66 These details are included: ‘Name’: both the CRD and the ECD require that the seller provide information regarding the name of the trader or service provider. The CRD at arts 5(1)(b) and 6(1)(b) requires that the trader provide identity and trading name. The ECD at art 5(1)(a) requires that the name of the service provider be provided to the consumer. ‘Contact information’: both the CRD and the ECD require that the seller provide contact information. Although the requirements are similar, the CRD requires that the seller provide ‘the geographical address at which he is established and his telephone number’. ECD art 5(1)(b). The ECD requires similar information, but does not require that a telephone number be provided (ie email address is sufficient) ECD art 5(1)(b)-(c).
67 For example, if the cost of using a distance communication is above a basic rate, the CRD requires that that cost be communicated to the consumer. CRD art 6(1)(f). The ECD requires that the seller provides the technical steps needed to conclude the agreement. ECD art 10(1). [Price] Both the ECD and the CRD have rules regarding price information to be provided to consumers. The ECD requires that the price term be ‘indicated clearly and unambiguously’ to the consumer. ECD art 5(2).
68 CRD arts 5(1)(c) and 6(1)(e).
69 CRD arts 5(1)(g) and 6(1)(r).
70 CRD arts 5(1)(h) and 6(1)(s).
of or can reasonably be expected to have been aware of. \(^71\) Additional information regarding applicable codes of conduct must also be provided pursuant to the CRD. \(^72\) However, the CRD does not specifically require any information regarding data security.

The above section has provided a cross section of sorts on the requirements of consumer protection law regarding the fairness of terms and informational requirements and the broad protections that are currently in place in the EU. Even with these considerable protections, further updates are being proposed to address how European consumers consume digital products. The next section considers the proposed legislation aimed at addressing digital products and its potential impact on cloud computing.

**A BRIDGE TOO FAR: ADDING DATA SECURITY REQUIREMENTS AND THE PROPOSED DIRECTIVE ON CONTRACTS FOR DIGITAL CONTENT**

Based on the existing framework, European consumers benefit from a great deal of protection when making purchases online. According to the DSM strategy, there is still much work to be done in building trust and expanding markets. In particular, the DSM strategy describes consumer contracting barriers as impediments to increasing online or cross-border trade. \(^73\) Expressly, there are areas—such as cloud computing contracts—where the rights and legal protections granted to European consumers have not been adequately represented. Following the abandonment of an omnibus Common European Sales Law (CESL) in 2014, which would have broadly addressed digital content, less expansive solutions were proposed. \(^74\) The proposals focused on two particular types of agreements, namely contracts for digital content and contracts for goods. \(^75\) This article focuses on the former.

The proposed Directive Concerning Contracts for the Supply of Digital Content (proposed DCD) is particularly relevant to cloud computing. \(^76\) The proposed DCD aims to eliminate the fragmentation currently taking place across EU Member States regarding protections provided to consumers purchasing digital content. Some jurisdictions, including the UK and the Netherlands, have adopted legislation applicable

---

71 CRD art 5(1)(h).
72 The ECD provides a similar requirement that ‘[a]ny relevant codes of conduct to which he [the trader] subscribes and information on how those codes can be consulted electronically’. ECD arts 10(2) and 16.
73 DSM (n 9) 4–5.
74 Hugh Beale QC, ‘Scope of Application and General Approach of the New Rules for Contracts in the Digital Environment’ European Parliament Rights and Constitutional Affairs (2016), 6 <https://polcms.scu.org.europarl.europa.eu/cmsdata/upload/4c6998e4-65fe-46e5-9006-8fa54b85e7f7/Beale.pdf> accessed 26 June 2016.
75 European Commission (EC), ‘Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee: Digital Contracts for Europe - Unleashing the Potential of E-commerce’ (Brussels) 9 December 2015 COM (2015) 633 final <http://ec.europa.eu/justice/contract/digital-contract-rules/index_en.htm> accessed 26 June 2016.
76 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content Brussels, 9 December 2015 COM (2015) 634 final, 2015/0287 (COD) (hereinafter ‘proposed DCD’ or ‘DCD’) <http://ec.europa.eu/justice/contract/files/digital_contracts/dsm_digital_content_en.pdf> accessed 26 June 2016.
to digital content.\textsuperscript{77} EU regulators worry that fragmentation could impact the willingness of users to purchase digital goods from other Member States, thereby hindering expansion of the DSM along with creating confusion among sellers regarding the applicable rules when offering content and services in other Member States.\textsuperscript{78} As proposed, the Digital Content Directive will be a ‘full harmonization directive’.\textsuperscript{79} Like the CRD, this will give it broad application across the EU with limited variance among Member States.\textsuperscript{80} The proposed DCD is designed to be mandatory and contract terms that attempt to exclude its application—to the detriment of the consumer—will not be binding on the consumer even if the term is accepted as part of the contract.\textsuperscript{81}

In addition to ‘typical’ digital content, including music and movies, the proposed DCD would apply broadly to digital content and services including cloud computing on either a pay-for-use or data-for-use basis.\textsuperscript{82} Over and above providing a more harmonized approach, the proposed DCD contains aspects that would address some of the problems singled out in cloud computing contracts. For instance, the proposed DCD has provisions involving long-term contracts, which have not been specifically regulated outside of the general ‘unfairness provisions’ of the UTD.\textsuperscript{83} Further, the proposed DCD would require that the digital content contained in the service is ‘in conformity with the contract throughout the duration of the contract’.\textsuperscript{84} If a dispute between supplier and consumer occurs, the burden is on the supplier to show that the digital content is in conformity with contract terms.\textsuperscript{85} By addressing some of the difficulties in proving a service did not function properly, the proposed DCD makes it easier for consumers to bring complaints. For example, if a consumer’s cloud service is not functioning properly, it is difficult for a user to prove non-conformance. Although the DCD provides a rather confusing/complex scheme regarding contract termination, by shifting the burden it places the consumer in a better position to bring a claim.\textsuperscript{86}

The proposed DCD would also require a high level of interoperability and portability for consumer data, thereby addressing what has been considered a major

\begin{footnotesize}
\begin{tabular}{l}
\textsuperscript{77} EC Unleashing the Potential of E-commerce (n 75) 3. See also [UK] Consumer Rights Act 2015 <http://www.legislation.gov.uk/ukpga/2015/15/pdfs/ukpga_20150015_en.pdf> accessed 26 June 2016.
\textsuperscript{78} Proposed DCD (n 76) Explanatory Memorandum, 2–3.
\textsuperscript{79} DCD art 4.
\textsuperscript{80} DCD art 4.
\textsuperscript{81} DCD art 19.
\textsuperscript{82} DCD art 2(1)(b-c). See also Recital 13 providing that ‘in the digital economy, information about individuals is often and increasingly seen by market participants as having a value comparable to money.’
\textsuperscript{83} DCD art 16 provides consumers with a clear right to terminate long-term contracts and to obtain their content from the provider. In addition to providing the means for a clean break, this provision combats the disadvantage consumers face under so-called ‘data hostage’ clauses that generally require that the consumer pay all debts and/or settle all disputes before data can be removed. Robert H Carpenter Jr, ‘Walking From Cloud to Cloud: The Portability Issue in Cloud Computing’ (2010) 6 Washington Journal of Law, Technology and Arts 9, 12–14.
\textsuperscript{84} DCD Recital 29.
\textsuperscript{85} DCD art 9. DCD Recital 32. Noting the difficulty consumers will likely have in proving non-conformity given the high-tech nature of digital content.
\textsuperscript{86} DCD art 13.
\end{tabular}
\end{footnotesize}
barrier to greater consumer usage of cloud computing. The proposed DCD also provides clearer requirements in areas of central concern for cloud computing users, including ‘accessibility, continuity and security’.\(^\text{87}\) In addition to providing consumers with rights throughout the duration of the contract, the proposed DCD gives consumers the benefit of a remedy when services fail. If a supplier fails to supply digital content, the proposed DCD gives the consumer the right to ‘terminate the contract immediately’.\(^\text{88}\) This addresses some of the often-cited concerns regarding lock-in or high exit costs for consumers.

From a consumer protection perspective, it can be argued that more layers of protection are always better. But is the proposed DCD needed to fill a void as either an instrument of harmonization or as a critical ‘gap filler’ providing essential legal protections? In other words, given the substantial protections outlined in Section 2, is the proposal a necessary evolution of the consumer protection regime regarding digital content or is it redundant?

In the following section, I evaluate problem areas for ‘common’ cloud computing contract terms, first, by applying the ‘law as it is’ under the current EU scheme and then the ‘law as it has been proposed’ under the proposed DCD. The focus is on security and other ‘fit-for-purpose’, ‘quality’ or ‘conformity’ aspects that might impact cloud contracts in the areas of data security and rights commonly reserved by CSPs regarding limitation of liability and variation of contract terms or services. The point of departure for the terms chosen is to evaluate three terms that either directly impact, or are adjacent to, data security concerns in that they have the potential to affect security and CSP liability for inadequate data security practices.\(^\text{89}\) Further, I evaluate how the contract clauses might be addressed within the framework proposed by the proposed DCD. Finally, this section provides some comparison with legal aspects of data security in the USA.

**Data security**

In the EU, current consumer protection legislation does not include specific requirements mandating adequate data security. Requirements for ‘adequate security measures’ impacting consumers are primarily found in the context of EU data protection law that places different levels of responsibility on parties depending on their role in the data processing relationship.\(^\text{90}\) Under the current regime, data ‘controllers’ have the ultimate responsibility for treating the personal data entrusted to them in conformance with legal requirements while processors work ‘on behalf of’ or ‘under the instruction of’ data controllers.\(^\text{91}\) Although the roles may change, in the typical cloud

\(^{87}\) DCD art 6(1)(a).

\(^{88}\) DCD art 11.

\(^{89}\) Studies conducted in Australia, the UK, and the USA have shown that the terms offered by CSPs are relatively consistent globally. Carol M Hayes, Jay P Kesan and Masooda N Bashir, ‘Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency’ (2013) 70 Washington and Lee Law Review 85; Mark Vincent and others, ‘Cloud Computing Contracts White Paper: A Survey of Terms and Conditions’ (2011) 21, 3–4; Bradshaw, Millard and Walden (n 53) 51–52.

\(^{90}\) 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 (‘95/46/EC’) art 17 and Recital 46.

\(^{91}\) 95/46/EC art 2(d) & (e). For additional analysis on security aspects, see Bygrave (n 7) 164–65.
computing scenario, the controller is the party using the cloud service, while the CSP is the processor.

Under the recently adopted General Data Protection Regulation (GDPR), entering into force in 2018, entities processing personal data will have increased accountability and data governance obligations on several fronts.\(^\text{92}\) This includes, among other obligations, a heightened duty of care on a controller's selection of processor and ability to demonstrate compliance.\(^\text{93}\) Importantly in the cloud computing context, the GDPR also places direct obligations on processors, often CSPs.\(^\text{94}\) In addition to other direct obligations, the GDPR limits the ability of processors to add subcontractors or subprocessors without consent from the controller.\(^\text{95}\) Among other requirements, these direct obligations will require processors to '... ensure a level of security appropriate to the risk...'.\(^\text{96}\) Furthermore, the GDPR will generally require entities processing personal data to provide more documentation and in some instances sharpen the security practices of their operations.\(^\text{97}\)

These requirements may translate into greater protections and security for consumer data stored in cloud services. However, in the limited areas where data protection law is not applicable, for example, the processing of non-personal data, CSPs would arguably not be obliged to provide security measures.\(^\text{98}\) That is not to say that there is 'no' application of EU consumer protection law to data security either directly or by implication in the existing legislation, since the 'unfairness test' and 'good faith' requirements provided in the UTD, as evaluated above, are applicable. Moreover, the service must be in conformity with the contract under the CRD.\(^\text{99}\) However, clear or direct requirements, informational or otherwise, for 'reasonable' or 'adequate' data security requirements are marginal in consumer protection legislation.

Member States have rules that apply to misleading or unfair data security practices. As noted by Cunningham and Reed, under the Unfair Terms in Consumer Contracts Regulations (UTCCR), CSPs have an obligation to provide transparent information about the levels of integrity and confidentiality they are providing to consumers.\(^\text{100}\)

---

\(^{92}\) 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 (GDPR) OJ L 119, 4 May 2016, 1–88. Responsibilities of Controller art 24, Accountability Principle art 5(2), Privacy by Design art 25, Increased Records of Processing Activities art 30, Security of Processing art 32, Notification of Data Breach art 33–34, Privacy Impact Assessments arts 35–36 and Designation of the Data Protection Officer art 37, among other obligations.

\(^{93}\) GDPR art 24. As the cloud user is generally the party making decisions regarding the 'purposes and means of the processing', they will be considered the data controller. See also GDPR art 28(1) '... the controller shall use only processors providing ... appropriate technical and organisational measures ...'.

\(^{94}\) GDPR arts 28 and 4(8).

\(^{95}\) GDPR art 28 (2). For further discussion on this problem under the current directive, see Kevin McGillivray, 'Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU', (2014) 17 Tulane Journal of Technology & Intellectual Property Law 217, 238–48.

\(^{96}\) GDPR art 28 (3)(c) requiring compliance with art 32.

\(^{97}\) GDPR art 32. See also art 5 (f) requiring ‘... appropriate security of the personal data, ...’.

\(^{98}\) The requirement that the data processed be personal for application is applicable in both the directive and the regulation. 95/46/EC art 3(1) and GDPR art 2, respectively.

\(^{99}\) CRD at 5(1)(e) requiring 'conformity for goods' and providing similar 'quality' requirements.

---
consumers.\textsuperscript{100} This is the case even when a subcontractor is providing the function and the CSP does not have complete control over all aspects of the service.\textsuperscript{101} The authors further note that CSPs should not advertise their service ‘…in a manner that raises a reasonable expectation on the part of consumers that data will be maintained as confidential and integral’.\textsuperscript{102} However, where a CSP does not provide misleading information or informs the consumer that the consumer is responsible for their data’s integrity and confidentiality, the provider’s obligations appear to be substantially reduced—although they still require that the service is ‘carried out with reasonable care and skill’.

Data security requirements are generally defined in the contract between the consumer and CSP, although the level of security is rarely framed with much specificity. This begs the question, should adequate data security be categorized as an ‘add-on’ or additional service bargained for in the contract or is adequate security incorporated as part of the service or content being offered? From another perspective, is a digital service offered without adequate or reasonable data security incomplete, considered not fit for purpose, or incompatible with the requirements of good faith?

In cloud computing services aimed at the mass consumer market, contract terms regarding data security are often vague and difficult to locate. A study by the research company Gartner found that ‘buyers of commercial cloud services, especially SaaS, are finding security provisions inadequate’.\textsuperscript{103} In a study of cloud computing contracts commissioned by the European Commission, researchers found no specific measures requiring data security in the consumer protection context.\textsuperscript{104} The study further noted that when such requirements were provided, it was often in the contract or part of a contract rider or other attachment.\textsuperscript{105} However, the report did not provide specific examples or point to local jurisdictions that had additional requirements regarding data security outside of a ‘draft’ German ‘IT Security Act’.\textsuperscript{106}

In a 2015 study of contract terms by Queen Mary University of London (QMUL) Cloud Legal Research Project, the researchers found that contract terms used to express security practices varied among providers.\textsuperscript{107} However, relatively non-specific terms were common, including ‘generally accepted’, ‘industry standard’, ‘reasonable’ or ‘commercially reasonable’.\textsuperscript{108} The QMUL study further noted that specific terms for data security were not always easy to locate within the contractual framework and the user was often required to search out specific pages, consult online help centres, or read the CSP’s privacy policy.\textsuperscript{109} In other words, data security

\textsuperscript{100} Cunningham and Reed (n 17) 356. The UTCCR implements the UTD (n 37) in the UK.
\textsuperscript{101} ibid.
\textsuperscript{102} ibid.
\textsuperscript{103} Press Release, ‘Gartner Says Cloud Contracts Need More Transparency to Improve Risk Management’ (Egham, UK, 1 August 2013) <http://www.gartner.com/newsroom/id/2567015> accessed 26 June 2016.
\textsuperscript{104} EC Contract Study (n 3) 57.
\textsuperscript{105} ibid.
\textsuperscript{106} ibid. Draft legislation may result in a German ‘IT Security Act’ including provisions that would safeguard a certain minimum IT security standard.
\textsuperscript{107} Kamarinou, Millard and Hon (n 6) 51–52.
\textsuperscript{108} ibid.
\textsuperscript{109} ibid 54–55.
policies or practices were not always accessible, and when found, they provided unclear descriptions regarding their level of protection.

The reason for providing little information can be explained to some extent on the nature of data security. Although common elements and approaches do exist, data security is provided on something of a sliding scale. One plan or standard for all users is neither commercially reasonable nor practical. Users storing highly sensitive information, such as medical or financial data, require, and are often willing to pay for, a more advanced system of protection. At the other end of the spectrum, most consumers are not interested in the ‘how’ behind data security—they just want to know that the system they are using is secure. In any case, terms such as ‘standard’ and ‘generally accepted’ are difficult to assess when industry practices or standards vary considerably.

When it comes to data security, there are good reasons for the lack of explicit detail in publically available information. Too much disclosure may negatively impact data security by providing would-be attackers with a blueprint of the measures in place. With standard contracts aimed at a mass market, overly specific security terms are cumbersome and may be difficult to rectify with some of the externalities of outsourcing that are common in cloud computing. For example, if subcontractors are delivering different parts of the cloud service, they may use varied security practices in their respective roles. Although varied, the different components of the service may provide adequate security even if approached differently at the various levels.

It may be difficult for a CSP to know and concretely enumerate all of the different security practices employed at the beginning of the service. Further, updating contract terms to reflect security changes made by partners during the service provides an additional challenge, and the data security landscape changes rapidly. A system that is secure—and meets industry standards—when the contract is entered into might not be secure six months or a year later if it is not monitored and updated. After all, data security includes a lot of moving parts from the logical side to the physical and requires an understanding of not only the technical aspects but also the people and places where the system is provided.

Looking at the other side of the Atlantic, in the USA, the regulatory approach to data security is generally ex post and there is no single omnibus federal law requiring data security. As noted by Stegmaier and Bartnick, the focus instead is on

110 Information security is not a ‘one size fits all’ calculation. Organizations must consider the specific threats they face while also assessing their individual security capabilities. Peter Sloan, ‘The Reasonable Information Security Program’ (2014) 21 Richmond Journal of Law & Technology 2, para 21 <http://jolt.richmond.edu/v21i1/article2.pdf> accessed 26 June 2016.
111 ibid para 22.
112 DCD at Recital 47. In recognizing the chain of providers often behind the supply of digital goods, the DCD requires that the supplier retains necessary rights or privity of contract in order to ‘... cover his liability towards the consumer.’
113 Sloan (n 110) 4.
114 Gerard M Stegmaier and Wendell Bartnick, ‘Psychics, Russian Roulette, and Data Security: The FTC’s Hidden Data-Security Requirements’ (2013) 20 George Mason Law Review 673, 673. Justin C Pierce, ‘Shifting Data Breach Liability: A Congressional Approach’ (2016) 57 William & Mary Law Review 975, 985–93 <http://scholarship.law.wm.edu/wmlr/vol57/iss3/6> accessed 26 June 2016.
criminalizing unauthorized access’. An FTC publication on the standard of data security that ought to be provided simply stated ‘[t]he [data security] standard is straightforward: Companies must maintain reasonable procedures to protect sensitive information. Whether your security practices are reasonable will depend on the nature and size of your business, the types of information you have, the security tools available to you based on your resources, and the risks you are likely to face.’ As a concept, reasonableness is well established in US information security law. However, the FTC standard as provided gives CSPs little information to understand the steps necessary for compliance. For example, if a provider has few resources available, should they categorically refrain from storing certain types of information such as sensitive personal information or financial data? How might this impact IaaS providers with little knowledge of the types of data stored in their systems?

A recent case from the USA sheds some light on the interface of data security consumer protection law. In FTC v Wyndham Worldwide Corp, the gap between the contract term, ‘industry standard’, and what was actually provided resulted in the term being adjudicated as unfair and misleading. In Wyndham, the FTC brought an action against the global hotel services provider ‘Wyndham’ for failing to provide adequate data security when storing its customers’ sensitive personal information. In fining Wyndham, the FTC determined that its privacy policy was inaccurate and deceptive; it had claimed to follow ‘industry standard’ data security practices and had asserted that it made ‘commercially reasonable efforts’ to provide adequate security, including utilizing well-established security technologies, such as encryption and firewalls, but it had not.

The FTC charged that data security practices actually used by Wyndham were so inadequate that the promises made in its privacy policy were misleading. As a result of the security gaps, attackers were able to access 600,000 items of unencrypted credit card information in Wyndham’s accounts on three separate occasions. The total cost of this stolen data and the instances of fraud, identity theft and related expenses for consumers amounted to over $10.6 million. Wyndham maintained that its security policies were sufficient and argued that the attacks were beyond its control. Wyndham appealed the fine levied by the FTC to the district court, and after being ruled against there, moved to the court of appeals.

The reviewing appellate court determined that the FTC has the authority to regulate cyber security as an unfair trade practice. In considering the unfairness claim, the court specifically pointed to the security practices that allowed multiple intrusions into Wyndham’s systems over a two-year period, focusing on problems with

115 Stegmaier and Bartnick (n 114) 673.
116 ibid 695.
117 Sloan (n 110) para 131.
118 [2015] 799 F 3d 236 (‘Wyndham’). 15 USC s 45(a) broadly prohibits practices affecting commerce that are ‘unfair’. Justin Brookman, ‘Protecting Privacy in an Era of Weakening Regulation’ (2015) 9 Harvard Law & Policy Review 355, 355–56.
119 Wyndham (n 118).
120 ibid 241.
121 For further discussion on the FTC’s authority to regulate cyber security practices, see Woodrow Hartzog and Daniel J Solove, ‘The Scope and Potential of FTC Data Protection’ (2015) 83 George Washington Law Review 2230–300, 2258.
the way data were stored in clear, readable, non-encrypted text, inadequate password requirements, lack of firewalls and the failure to install security updates for a period of over three years.\textsuperscript{122} Additionally, Wyndham did not adequately restrict access by subcontractors or third-party vendors to its network or servers, granting many users wide access to its systems.\textsuperscript{123} Wyndham placed much of the blame for the failure of its systems on sophisticated hackers.\textsuperscript{124} However, given its lax security practices, it appears that a great deal of sophistication was not required.

The case is significant in that although the FTC has previously found privacy practices unfair, this is the first case where a court has reviewed the FTC’s authority to regulate data security as an unfair trade practice.\textsuperscript{125} Companies generally face problems with the FTC when they make a promise to take an action and then fail to follow through or contradict their promise to the consumer in some other way. However, unlike general data collection or billing practices, here, the FTC specifically considered certain cyber security practices to be ‘unfair’ based on their privacy policy’s promises of ‘industry standard’ security.

Wyndham essentially argued that there was no defined ‘industry standard’ and raised issues regarding ‘fair notice’ of data security requirements by the FTC.\textsuperscript{126} However, the appellate court also disagreed, finding the FTC was not required have officially provided standard or reasonable cyber security practices on a prior basis in order for Wyndham to be in breach. The court based its reasoning in part on other cases where the FTC had publicly levied fines against providers in the cyber security area and determined that such enforcement was not a complete surprise or ‘out of the blue’. As the court noted:

> As the FTC points out in its brief, the complaint does not allege that Wyndham used weak firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use any firewall at critical network points, did not restrict specific IP addresses at all, did not use any encryption for certain customer files, and did not require some users to change their default or factory-setting passwords at all...\textsuperscript{127}

The Court did not provide that any specific data security plan must be in place. However, Wyndham ‘should consider the probability and magnitude of harms to consumers caused by its data security practices and whether these costs outweighed any savings from not employing more secure practices’.\textsuperscript{128} This approach is in line

\textsuperscript{122} Wyndham (n 118) 240–42.
\textsuperscript{123} ibid 241. A common legal requirement for information security is that the provider safeguards information provided to third parties, as required by various US state and sector-specific federal laws. See Sloan (n 110) 81–86.
\textsuperscript{124} Wyndham (n 118) 242.
\textsuperscript{125} The Harvard Law Review Association (HLRA), ‘Administrative Law—Federal Trade Commission Act—Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice Of Potential Liability FTC v. Wyndham Worldwide Corp., (2015) 799 F.3D 236’ (2016) 129 Harvard Law Review 1120, 1123.
\textsuperscript{126} For further explanation of fair notice requirements in the Wyndham context, see Stegmaier and Bartnick (n 114) 698–702.
\textsuperscript{127} Wyndham (n 118) 256.
\textsuperscript{128} HLRA (n 125) 1123. Citing Wyndham (n 118) 256.
with general information security philosophy. Taking even minor steps, such as encrypting data and using strong passwords, would not have been prohibitively expensive yet would have benefitted the consumers immensely. After all, the data stored were sensitive credit card information carrying a clear potential for harm to consumers if exposed.

Evaluating the Wyndham case in an EU context, similar questions regarding the requirement to provide a certain level of data security are also apparent. Although this case exemplifies a negligent provider, consumers in the EU might also have difficulty showing that a CSP breached ‘industry standard’ practices when standard—or even prudent—data security requirements are not explicitly provided in most agreements. Although the CRD has relatively vast informational requirements, detailing—or even outlining information security practices—are not among them. The UTD also provides that contract terms that are unfair will not be enforceable against consumers pursuant to the UTD. However, the question remains, are absent or vague data security promises inherently unfair to consumers? For the actual security practices to be considered unfair or inconsistent with good faith requirements, must the contract terms promise more than ‘best efforts’? When contract terms specifically place the burden of security and resulting data loss on consumers, what protections are in place for the consumer?

This is not to say that the European consumer is without remedy or recourse. After all, given the broad provisions of the UTD, the requirement that CSPs provide ‘plain’ or ‘intelligible’ contract terms and that terms contrary to the requirement of ‘good faith’ will not be enforced against the consumer are certainly applicable. Although not particularly surprising for a directive from 1993, the UTD Annex of ‘blacklisted’ terms does not specifically address contract terms related to data security.

The proposed DCD does contain some additional protections potentially applicable to data security. The DCD obliges that digital content be provided to a certain ‘quality’ and includes a ‘fit for purpose’ requirement. Specifically, the proposed DCD also requires that:

In order to conform with the contract, the digital content shall, where relevant:
(a) be of the quantity, quality, duration and version and shall possess functionality, interoperability and other performance features such as accessibility, continuity and security, as required by the contract including in any pre-contractual information which forms [an] integral part of the contract; ...  

If the contract is silent on security requirements, the proposed DCD supplies such a term on an objective basis requiring that the digital content shall be fit for the purposes for which digital content of the same description would normally be used

129 Sloan (n 110) para 63.
130 UTD art 3(1). Recall also that this fairness test, and what is considered to be unfair regarding consumers, varies among Member States. Yuthayotin (n 46) 116. Discussing the varied application of UTD 3(1) when evaluating fairness.
131 DCD art 6(1)(b) and art 6(2).
132 DCD art 6(1)(a).
including its functionality, interoperability and other performance features such as accessibility, continuity and security, . . . \(^{133}\)

Although the proposed DCD does not state what is considered normal use with regard to security, the requirement is on a sliding scale of sorts. In determining the level of security the provider is required to provide, the DCD considers whether the services were provided on a ‘payment-for-use’ or ‘data-for-use’ basis—although both are covered by the DCD.\(^{134}\) In addition to remuneration, aspects such as ‘international technical standards,’ and when such standards are unavailable, ‘applicable industry codes of conduct and good practices’ are also relevant in determining what is normally required.\(^{135}\)

The template for determining what will occur in cloud computing services relies primarily on the contract terms agreed to by the parties. The DCD does not provide model or obligatory terms or contain an Annex similar to that in the UTD, and works as a ‘gap filler’ in the contract. In other words, the potentially more exacting standard for security practices in Article 6(2) will only be applicable if security practices are not stipulated in the contract. If the parties ‘agree’ to a low level of security, and the level of security delivered to the consumer is in conformance with what is provided in the contract in a ‘clear and comprehensive manner’, arguably a CSP will not be in breach for providing security that would normally be considered below the standard supplied per Article 6(2). As such, it seems advantageous for the CSP to provide some information on security practices in order to avoid having to conform to the objective standard requirement for security stipulated in Article 6(2). The CSP would still have to ensure consistency, and that the service is fit for purpose. However, with CSPs being able to avoid the potentially more exacting standard for security in Article 6(2) relatively easily, Article 6 in fact leaves the consumer with very little additional protection with regard to security.

Determining when contract terms such as ‘security’ have not been provided in a ‘clear and comprehensive manner’, and requiring that terms be supplied to the service, creates challenges based on current disclosure practices.\(^{136}\) For example, how might terms like ‘commercially reasonable’ data security be interpreted under Article 6? Is the term stipulated ‘in a clear and comprehensive manner’? Would a reviewing court apply the ‘would normally be used’ standard in DCD Article 6(2) or is the CSP granted a level of deference? The breadth of application of Article 6 has the potential to significantly add to the information CSPs must provide in contracts.

In addition to the more objective requirements, like technical standards, more subjective informal measures can also be considered, including ‘any public statement made by or on behalf of the supplier or other persons in earlier links of the chain of

---

\(^{133}\) DCD Recital 25 (emphasis added).

\(^{134}\) DCD art 6(2)(a). Jansen and Grance (n 60) 6.

\(^{135}\) DCD art 6(2)(b). See also Recital 28. Providing that suppliers should make use of ‘standards, open technical specifications, good practices and codes of conduct...’. For a discussion of a newly established ISO standard for cloud computing, see Paul de Hert, Vagelis Papakonstantinou and Irene Kamara, ‘The Cloud Computing Standard ISO/IEC 27018 Through the Lens of the EU Legislation on Data Protection’ (2016) 32 Computer Law & Security Review 16–30.

\(^{136}\) DCD art 6(2).
transactions . . . [.]\(^{137}\) Although this provision is relevantly imprecise, one could imagine that it applies to advertisements in addition to traditional public statements or statements made in conjunction with the sale. After all, there is some disconnect between the security showcased in advertisements by CSPs and the actual level of security promised in contract terms.\(^{138}\) For example, when cloud computing services claim to be ‘automatic,’ ‘unlimited’ or make other statements regarding their level of security or safety, these statements could be imposed on the CSP under this provision.\(^{139}\) The ‘public statement’ standard seems primarily focused on misleading statements and does include some exceptions. However, they require subjective fact-intensive analysis such as:

(i) he [supplier?] was not, and could not reasonably have been aware of the statement in question; (ii) by the time of the conclusion of the contract the statement had been corrected and; (iii) the decision to acquire digital content could not have been influenced by the statement.\(^{140}\)

Determining whether a statement could have influenced a consumer or that a supplier was not aware of a statement requires a fact-based analysis. Although the word ‘reasonable’ suggests that an objective standard will be applied, under what circumstances can a CSP no longer ‘reasonably’ claim to have been unaware of potentially misleading advertisements or statements by its sellers? The provision allows a CSP to rebut the presumption that its suppliers’ statements should be incorporated into its contract with consumers. However, the application of this standard and the scope of eventual protections it may provide consumers are unclear. If applied broadly, it may substantially impact current marketing practices.

**Limiting liability, disclaiming warranties and modification of contract terms in the cloud service**

Wide disclaimers of warranties and liability are common in many CSP agreements, particularity those offering ‘free’ services.\(^{141}\) When accepting these offerings, consumers often agree to oppressive contract terms that limit their ability to sue and recover losses under almost any circumstances, including data security failures.\(^{142}\)

---

\(^{137}\) DCD art 6(2)(b) (emphasis added).

\(^{138}\) For example, the CSP Amazon marketed their services to ‘confine customer data to regional zones’. However, regional storage was not described in the contract. Cunningham and Reed (n 17) 357.

\(^{139}\) McGillivray (n 95) fn 188. The UK Advertising Standards Authority (ASA) found use of the term ‘unlimited’ misleading when referring to data storage plans that were, in practice, effectively limited by server capacity. Cunningham and Reed (n 17) 339.

\(^{140}\) DCD art 6 (2)(c)(i-iii). Use of personal pronouns in the DCD referring to providers or sellers as ‘he’ or ‘him’ creates some confusion as personal pronouns are often associated with a living person—often a consumer—rather than a legal person such as a CSP.

\(^{141}\) Andrew Joint and Edwin Baker, ‘Knowing the Past to Understand the Present—Issues in the Contracting for Cloud Based Services’ (2011) 27 Computer Law & Security Review 9, 412–13. Timothy J Calloway, ‘Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm’ (2012) 11 Duke Law & Technology Review 12, 163.

\(^{142}\) Mandatory, or, as they are sometimes called, ‘forced arbitration clauses’ are a growing trend in contracts for digital goods and other online offerings, including cloud computing. See James R Bucilla II, ‘The Online Crossroads of Website Terms of Service Agreements and Consumer Protection: An Empirical
Based on QMUL’s findings, among others, USA-style total disclaimers of liability and warranties are problematic when applied in B2C transactions in the EU.\textsuperscript{143} Although some limits, such as a cap on damages, may be acceptable assuming that the amount is not too low, wide disclaimers of all responsibility will not.\textsuperscript{144} The CSP will be required to use reasonable care and make reasonable decisions regarding the data consumers store on their service; if not, it can expect to incur liability, regardless of the contract terms.\textsuperscript{145}

In the context of data security, it is unlikely that such disclaimers will be enforceable against European consumers. The proposed DCD would add a layer of protection by making the supplier of digital content liable for failure to supply the content or if the content does not conform as contracted.\textsuperscript{146} Furthermore, if the digital content is to be supplied over a period of time, the DCD requires that it be in conformance for the duration.\textsuperscript{147} For CSPs, this means monitoring and improvements to keep abreast of security threats.

Additionally, many terms offered by CSPs reserve the right to modify the terms of the agreement unilaterally.\textsuperscript{148} Variation or modification often applies to the terms of service and privacy policies, among other aspects of the service.\textsuperscript{149} Many of these changes are essential, such as software or security updates benefiting the consumer. Others, such as data collected or used for tracking or advertising, have the potential to constitute substantial alterations.

For consumers, if the contract is never really ‘final’ and requires active monitoring, it is unrealistic that consumers will receive, understand, and appreciate the changes. After all, as has been determined by several studies, it is rare that consumers read the terms the first time they are presented.\textsuperscript{150} Requiring that the consumer read the contract regularly enough that they become ‘fluent’ in the contract and are able to spot and appreciate differences among versions is unrealistic.

Contract terms allowing major one-sided alterations to the agreement will generally be considered unfair per the UTD.\textsuperscript{151} Although variation clauses are found in many cloud computing contracts, these amendments are limited to actions that are ‘reasonable’ and not ‘surprising or substantially unfair’ based on the original agreement in European jurisdictions.\textsuperscript{152} More concretely, the UTD provides that allowing

\begin{flushright}
Study of Arbitration Clauses in the Terms Of Service Agreements for the Top 100 Websites Viewed in the United States’ (2014) 15 Wake Forest Journal of Business and Intellectual Property Law 45. Jeremy B Merrill, ‘One-Third of Top Websites Restrict Customers’ Right to Sue,’ New York Times (23 October 2014) <http://www.nytimes.com/2014/10/23/upshot/one-third-of-top-websites-restrict-customers-right-to-sue.html?abt=0002&abg=0&_r=0> accessed 26 June 2016.
\end{flushright}
the seller or supplier to alter the terms of the contract unilaterally, without a valid reason specified in the contract, is unfair.\textsuperscript{153}

The DCD recognizes that digital content requires updates and modifications that often benefit the consumer.\textsuperscript{154} However, if the alterations ‘adversely affect access to or use of the digital content by the consumer’, the DCD sets some limits to the alterations to accessibility and security.\textsuperscript{155} Specifically, the contract must provide for modifications, the consumer must be notified ‘reasonably in advance’ with ‘explicit notice’, and the consumer must be allowed to terminate the contract without cost within 30 days of the notice.\textsuperscript{156}

The DCD provisions would allow CSPs to make necessary security alterations, but also provide the consumer with the information they need to evaluate changes that go beyond updates needed to keep the service running. Given the long-term nature of cloud computing contracts where a consumer could use the service for decades, this provision provides an avenue to make alterations without taking advantage of consumers. Although protections are available for cloud users under the UTD, those provisions seem to envision a one-off type sale rather than an ongoing relationship. This is perhaps an area where contract terms are unclear and the proposed DCD might add an important layer of statutory consumer protection.

**CONCLUSION**

In 2012, the European Commission released its report on unleashing the potential for cloud computing in Europe.\textsuperscript{157} The report focused heavily on ‘problems with contracts’, outlining existing areas as unsafe or problematic for consumers adopting cloud computing.\textsuperscript{158} The European Commission placed particular focus on terms limiting provider liability, user rights, and dispute resolution—without discussing security aspects of contract terms.\textsuperscript{159} The proposed DCD, to some extent, addresses data security in consumer contracting for cloud services and potentially takes some of the steps toward ‘safe and fair’ contracting terms outlined by the European Commission in its ‘unleashing’ document. However, the proposed DCD grants a high level of deference to CSP contracts and also uses relatively ambiguous terms (eg ‘normally be used’) to describe security levels.

Methods of providing less opaque security practices are not limited or confined to a choice between ‘private’ contractual means or ‘public’ legislative regulation. Such a narrow scope is neither feasible nor desirable. In addition to legislative mandates, self- and co-regulatory aspects may also play an important role in providing more consistent or visible security practices. For example, the International Standards Organization (ISO), working with many stakeholders, created standard ISO/IEC 27018, which is intended to address many of the privacy and security issues specific to cloud computing including some risks flowing from the asymmetrical consumer/
CSP contracting relationship. Unlike legislation, the standard outlines specific security and auditing practices that would provide consumers with assurances that a certain level of security is in place. However, given the added expense of adopting such standards, if they are not legally required, consumers may have a difficult time negotiating with CSPs and obtaining such terms.

Nevertheless, like creating a set of model contract terms for all CSPs, creating rigid security requirements is challenging. Although many public cloud services aimed at consumers are widely accessible, they are not fungible. Cloud computing services may be aimed at distinct types of users, utilize diverse software, and are made up of different partners and subcontractors resulting in dissimilar structures or layers. Perhaps one of the challenges in articulating data security practices—and functionality of digital goods more generally—is the manner in which security practices are developed and applied. Data security standards often begin as collections of trial and error leading to agreement among technologists. In the race to remain secure, things may change quickly; a practice that is considered safe in mid-September might be considered negligent by late October. This is not to say that guide points should be abandoned or that CSPs should be excused from making any specific promises to consumers. For example, requiring that data be encrypted, employing role-based access and enforcing firewalls, among other core security practices, are unlikely to vanish. Making promises in these areas will still provide CSPs with room to manoeuvre and deliver their services effectively.

Data security is a complex topic falling under many potential regulatory areas. As data protection law has recognized for some time, data security plays a crucial role in protecting users and maintaining their fundamental rights. Although EU data protection legislation also uses the same relatively non-specific requirements, it places a clear burden on CSPs to provide security. Currently, the level of data security being provided to consumers is extremely variable. Although low-budget applications and services often shoulder much of the blame, as the Wyndham case shows, big players do not always live up to expectations. Although the EU provides a strong lifecycle of consumer protection, if data security requirements remain outside of the consumer protection scheme, it is at the peril of consumers. Therefore, efforts to provide clearer information and data security standards in contracts are important steps in protecting consumers as the delivery of goods and services continues to change.

160 de Hert, Papakonstantinou and Kamara (n 135) 23–24.
161 ibid 25. Providing a ‘. . . comprehensive set of controls regarding information security policies, organisation of information security including asset management, asset control and cryptography’.
162 Jatinder Singh and others, ‘Twenty Cloud Security Considerations for Supporting the Internet of Things’ (2015) 99 IEEE Internet of Things Journal 1–16, 2 <http://ieeexplore.ieee.org/document/7165580/?reason=concurrency> accessed 26 June 2016. Roger Clarke, ‘Data Risks in the Cloud’ (2013) 8(3) Journal of Theoretical and Applied Electronic Commerce Research, 59–73 <http://www.rogerclarke.com/II/DRC.html> accessed 26 June 2016.