Response to Justice Select Committee's Call for Evidence on the EU Data Protection Framework Proposals

Cloud Legal Project
17 August 2012

1. This response is by Christopher Millard, Alan Cunningham and Kuan Hon, Cloud Legal Project (**CLP**)[1] http://cloudlegalproject.org**,** Centre for Commercial Law Studies, Queen Mary, University of London.[2] We have researched cloud computing since 2009. The Annex describes cloud computing and our research's scope.
2. Cloud computing's potential importance is recognised.[3] Data protection laws considerably affect cloud computing. This response, based on our research, addresses the proposals' impact on cloud computing from both service providers' and users' perspectives (but not how they might affect Queen Mary, University of London as an institution, ourselves as individuals using cloud computing in professional or personal capacities, or any specific body of users or providers).
3. **Summary.**

- Overall, we welcome the intention to clarify and modernise data protection rules.
- Our comments aim to minimise unnecessary regulatory burdens, complexity and uncertainty for the developing cloud industry and, indeed, burdens - whether direct or passed on via cost or other means - for potential cloud users.
- We understand prospective cloud users must comply with data protection laws, but believe there are more effective (and less burdensome) ways of encouraging industry development while addressing user concerns, such as raising awareness of secure encryption options, and fostering and supporting parallel development of industry standards and certification systems regarding data privacy and security. We therefore welcome proposals in these areas (including privacy by design and privacy by default) as a positive attempt to encourage best industry practice, which could help promote trust amongst actual and potential users. However, further clarification and guidance on those provisions is needed.
- The table below compares key issues under the current regime and the proposals. We believe they are crucial both for the cloud sector and cloud users, and need addressing.

Issue	Data Protection Directive	Proposals
1. Scope of 'personal data'	Existing laws only apply to 'personal data'. Currently, much data in the cloud are considered 'personal data', whatever the practical likelihood of identification or risk or likely extent of harm. This creates unnecessary burdens for many providers.	The proposals would not reduce the likelihood of much cloud data being considered 'personal data' under data protection law. If anything, they may increase it, further increasing burdens on providers.
2. Nature of cloud services	Existing laws treat providers as either data processor or data controller (or both). But infrastructure providers with little or no knowledge of, or control over, use of personal data, may essentially be neither, but merely passive intermediaries.	The 'either processor or controller (or both)' model is maintained. A more nuanced definition of 'processor', or exemption for providers acting as passive intermediaries, would be welcomed.
3. Determining	Existing laws do not adequately	Non-EEA providers and users may

[1] The CLP team comprises: Prof. Christopher Millard, Prof. Chris Reed, Prof. Ian Walden, Dr. Julia Hörnle, Dr. Alan Cunningham, W Kuan Hon and Simon Bradshaw.

[2] The Cloud Legal Project was made possible as a result of generous charitable donations from Microsoft Corporation. These views, however, are the independent views of the research team.

[3] Commissioner Kroes has expressed the desire to 'remove obstacles – and indeed give a boost – to a competitive and effective cloud market'. Neelie Kroes, EU Data protection reform and Cloud Computing, Microsoft Executive Briefing Centre Brussels, 30 January 2012.

jurisdictional matters	reflect many cloud arrangements' logistics, determining jurisdiction based on 'establishment' of the controller or use of equipment in the EEA. This may discourage establishment and/or use of EEA-based cloud infrastructure or services.	still become subject to data protection rules simply through using an EEA data centre or provider. While we welcome the proposed 'offering goods or services' test, further clarification is required on the derogation's scope.
4. International transfers of personal data outside the EU	Existing laws focus unduly on data location, rather than restricting unauthorised access to intelligible data.	Additional restrictions on transferring personal data to third countries. A new derogation - for transfers not 'frequent or massive', necessary for the legitimate interests of the controller or processor - is welcome. However, the 'frequent or massive' concept is unclear, and seems unnecessary.
5. Law enforcement access to data in cloud environments	Existing laws may render disclosure to non-EEA law enforcement agencies unlawful, creating much legal uncertainty for users and providers.	Existing uncertainties are perpetuated. Clarification would be welcomed.
6. New issue for cloud: Increased bureaucracy and compliance burdens		New requirements on data protection impact assessments, consultation with regulators, data protection officers and detailed documentation.
7. New issue: Increased role of supervisory authorities		Increased regulatory oversight. While there is a clear case for improving transparency, security and accountability, providers who are mere intermediaries may be subject to inappropriate regulation.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

4. **Overview.** In cloud computing, we consider the proposals would not strike the right balance between effective data protection and regulatory, financial and administrative burdens. Indeed, they may increase burdens without necessarily improving data protection, because the proposals would not resolve certain existing problems (outlined further below), but would compound some of them.
5. **'Personal data'.** The proposals would not clarify sufficiently the 'personal data' definition, which is the trigger for applying EU data protection laws. Currently, much cloud data are 'personal data', to which the regime applies irrespective of availability of secure encryption, practical likelihood of identification, or risk or likely extent of harm. This is an unnecessary regulatory burden, particularly on providers. We believe alternative tests of likelihood of identification/risk and likely extent of harm would better reflect technological and logistical realities of cloud business/technology models and use. Also, the proposals should address specifically the role of encryption and the status of encryption or anonymisation processes and encrypted data.
6. **Nature of cloud services**. Currently certain providers, who may merely provide infrastructure services (facilities and/or tools) to be used autonomously by end-users or intermediate platform or service providers ('infrastructure providers'), are nevertheless subject to data protection rules. Instead of recognising the nature, complexities and nuances of cloud services, the proposals would perpetuate the binary 'controller'/'processor' distinction and impose new obligations and liabilities on 'processors', such as requirements regarding provisions in controllers' contracts with processors, many of which ill suit cloud services models.[4] This may obstruct development of multi-layered cloud services, particularly for market entrants wishing to establish data protection-compliant services using third party platforms or

[4] See table in Annex.

infrastructure, which may reduce users' market choice. We recommend a more nuanced definition of 'processor', and/or modernising and extending E-Commerce Directive exemptions to cloud services whose providers are merely passive intermediaries, and who should therefore benefit from that Directive's intermediary immunities (unless and until acquiring the requisite knowledge and control regarding personal data processed by customers using their resources). Development and legal recognition of suitable industry standards and certifications could help address concerns regarding providers and sub-providers.

7. **Jurisdictional matters.** While we welcome proposals to abolish 'means' / 'equipment' tests and base data protection jurisdiction on targeting, we consider that, for legal certainty, the meaning and scope of the proposed terms and definitions need clarification, particularly 'offering', 'only occasionally', 'monitoring' and 'main establishment'. The concept of 'directing' is better understood than 'offering'. Currently, providers and users risk becoming subject to data protection rules if they use an EEA data center or EEA provider, without sufficient clarity as to which Member State's regulator has authority over them. This may disincentivise non-EEA users from using EEA providers or data centers. The proposals would perpetuate and indeed exacerbate these problems, given proposed extensions of data protection regulation to personal data processing in the context of activities of a *processor's* EEA establishment, without exemptions for cloud intermediaries. Finally, the proposals would not close a loophole, discussed in our research,[5] which may undermine protection for some EU residents when using services of non-EEA providers.
8. **International transfers of personal data outside the EU**. Given the ease of remote access and data transfers in the internet age, we consider that security, accountability and transparency are more important, in terms of effective privacy, than data location. We argue the focus should be on restricting unauthorised access to intelligible data, rather than restricting international data transfer *as such*. For example, where data are securely protected via strong encryption, focusing primarily on their geographical location may be unnecessary and may restrict inappropriately use of cloud services. Ease of data transfer to third countries can facilitate considerably development and efficient use of cloud services. The proposals would, rather than making data location simply one element affecting security, impose additional restrictions regarding transfer of personal data to third countries, including requiring regulatory approval. This would increase regulatory burdens on EU businesses using cloud services involving personal data transfers to third countries, compounding current difficulties. A proposed derogation for transfers to a third country necessary for 'the purposes of the legitimate interests pursued by the controller or the processor' might be helpful, but would not apply to transfers that are 'frequent or massive', and thus would not assist cloud computing. We argue the focus should be on appropriate safeguards, rather than size or frequency of transfers. Legal recognition of appropriate industry standards and certifications could allow security to be maintained while allowing international transfers.
9. **Law enforcement access to data in cloud environments.** Uncertainty regarding law enforcement access to data in cloud environments may discourage cloud adoption. Current laws permit processing for law enforcement purposes, and exempt certain processing from some data protection obligations where necessary for reasons including 'the prevention, investigation, detection and prosecution of criminal offences'. However, where an EEA provider responds to a request for personal data from a *non*-EEA law enforcement agency, transfer of data outside the EEA must be legitimate under data protection rules. Absent 'adequacy', the Directive's Article 26 offers certain exemptions, but the relevant exemption's scope is also uncertain. Current laws may, therefore, render disclosure to non-EEA law enforcement agencies unlawful. The resulting legal uncertainties for users and providers could deter take-up of cloud services.
10. **Increased bureaucracy and compliance burdens.** The proposals are likely to increase bureaucracy and compliance burdens for controllers and processors. As infrastructure providers are likely to be considered 'processors' - while being, in reality, merely passive intermediaries – we believe these expanded responsibilities would be inappropriate; for example, impact assessments, and new record keeping responsibilities. While there is a clear case for promoting accountability, security and transparency in the cloud, greater flexibility may be required to facilitate cloud services development and accommodate industry standards, especially for those infrastructure providers we believe should be considered neither controller nor processor.
11. **Increased role of supervisory authorities**. The proposals expand data protection supervisory authorities' role. For example, the national supervisory authority of the country that is the 'main establishment' of a cloud provider would be competent to supervise its processing activities in all Member States (proposed Article 51). Furthermore, controllers and processors must consult and seek authorisations from national supervisory authorities for certain personal data processing, for example many data transfers to third countries (proposed Article 34). Again, we welcome initiatives to promote a

[5] Annex, 2.4.

cloud environment where transparency, security and accountability are the norm. We are concerned, however, that infrastructure providers will also be unnecessarily subject to this increased regulatory oversight. Clarification here would be welcome.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

12. The Summary's 'next steps' are at a high level. We support the proposal to resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals, if it addresses the cloud issues outlined above at a detailed level.

Annex

1. Cloud computing - definition and differences

The CLP definition is:

- Cloud computing provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in relation to demand.
- Services (especially infrastructure) are abstracted and typically virtualized, generally being allocated from a pool shared as a fungible resource with other customers.
- Charging, where present, is commonly on an access basis, often in proportion to resources used.

Cloud service models[6] are often categorised as Infrastructure as a Service ('IaaS') (providing computing resources like processing power and/or data storage), Platform as a Service ('PaaS') (providing tools for developing and deploying custom applications, eg certain mobile applications), or Software as a Service ('SaaS') (providing end user applications, like webmail or online word processing).

Current laws, and the proposals, envisage traditional outsourcing and stand-alone databases (in use when current laws were drafted). They do not cater adequately for key differences arising from service type, particularly with public shared-infrastructure IaaS and PaaS (ie infrastructure services), or differences arising from individual services' designs:

Traditional assumptions	Cloud computing
1.1 Active agent, vs self-service usage	
Traditional outsourcing: controller hires processor, who actively processes data for controller according to controller's instructions.	Controller rents IT resources from provider. Controller processes data in self-service fashion, using infrastructure/resources supplied by the provider - as when renting computers. Many infrastructure providers do *not* actively act as agent processing data for controller, but at most passively store data the controller has chosen to store on the provider's infrastructure. Current requirements for providers to follow controllers' 'instructions' in processing data make little sense with infrastructure services where the *controller* - not provider - processes data, using the provider's resources. Providers maintain standardised infrastructure and environments for users' data processing. If users can specify setup of shared infrastructure (eg security-related measures), this undermines the cost-saving commodity characteristic of cloud; also, it may be impossible for providers to comply if different users' instructions conflict. The underlying concerns are that providers or others could (1) access intelligible data, or (2) undermine data integrity. On (1), see 3. below. On (2), controllers may backup internally or to other cloud services. On both, certifying services' security to minimum industry standards seems more workable for facilitating risk assessments than 'instructions' requirements, particularly as many users lack technical expertise.
1.2. 'Direction of travel' and sequence of events	
Controller hires processor to meet controller's specific processing needs. Processor may engage sub-processors to assist with its processing duties.	Provider offers pre-packaged commoditised services (sometimes built atop third party services, usually on the third party's standard terms). Controller chooses the provider and pre-built package for its specific processing and other needs. Customisation is sometimes possible, but costs extra time/money.
1.3. Data location and data deletion, vs access to intelligible data	
With stand-alone databases, eg on tape drives, where data are unencrypted or insecurely encrypted, whoever physically holds the media may access stored data upon knowing the file format (to interpret the 1's and 0's). Media location therefore affects security.	Given distributed storage and proprietary file formats, access to physical media, eg storage hardware in a third country, does not necessarily afford access to intelligible data. The only sure way to access intelligible data is through the user logging in to reunite fragments into intelligible form automatically. Fragments are distributed automatically; providers may or may not know in which hardware all fragments comprising one data set are stored. Some fragments may be intelligible, others not. Some providers can bypass or use customer logins, others cannot. Even providers bypassing customer logins cannot, without decryption keys,

[6] Mell and Grance, The NIST Definition of Cloud Computing (2011).

	decipher data securely encrypted by controllers. Similarly, after deletion operations, fragments may or may not be intelligible or re-unitable. Again, these depend on service type and design.
1.4. User control	
Controller closely controls processing.	Cloud services differ. Users do not necessarily lose all control in the cloud; they may encrypt data, IaaS users may install firewalls, system design may affect what's controllable. Regulating all cloud services alike, as if they posed equal risks to privacy, could impede cloud development and use.
1.5 Security	
Controller dictates security requirements.	See 1.1. Some regulators acknowledge that too much disclosure about shared infrastructure may undermine security.

2. CLP research to date on the following legal implications of cloud computing

2.1 Standard contract terms[7] - surveyed 31 standard contractual terms and conditions of US and European cloud providers.
2.2 Negotiations of changes to standard terms[8] - based mainly on detailed interviews with UK and global cloud providers, customers and others.
2.3 UK G-Cloud v1 and cloud contracts.[9]
2.4 Determining data protection jurisdiction.[10]
2.5 Scope of 'personal data'.[11]
2.6 Nature of cloud service under data protection laws.[12]
2.7 International data transfers in the cloud under data protection laws.[13]
2.8 Information ownership.[14]
2.9 Competition law issues.[15]
2.10 Law enforcement access to cloud data.[16]

[7] Bradshaw, Millard, and Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services (2010) http://ssrn.com/abstract=1662374.

[8] Hon, Millard, and Walden, Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now (2012) http://ssrn.com/abstract=2055199.

[9] Hon, Millard, and Walden, UK G-Cloud v1 and the Impact on Cloud Contracts (2012) http://ssrn.com/abstract=2038557.

[10] Hon, Hörnle, and Millard, Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3 (2012) http://ssrn.com/abstract=1924240.

[11] Hon, Millard, and Walden, The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1 (2011) http://ssrn.com/abstract=1783577.

[12] Hon, Millard, and Walden, Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2 (2011) http://ssrn.com/abstract=1794130.

[13] Hon and Millard, Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the EEA? The Cloud of Unknowing, Part 4 (2011) http://ssrn.com/abstract=1925066.

[14] Reed, Information 'Ownership' in the Cloud (2010) http://ssrn.com/abstract=1562461.

[15] Walden and Luciano, Ensuring Competition in the Clouds: The Role of Competition Law? (2011) http://ssrn.com/abstract=1840547.

[16] Walden, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent (2011) http://ssrn.com/abstract=1781067.