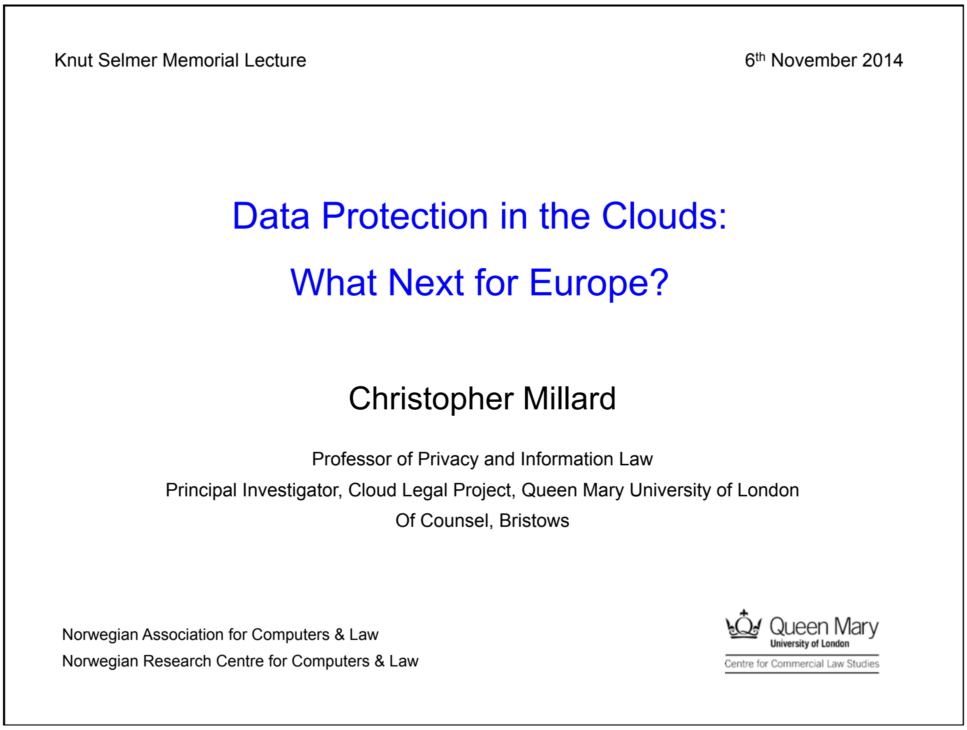


Knut Selmer Memorial Lecture

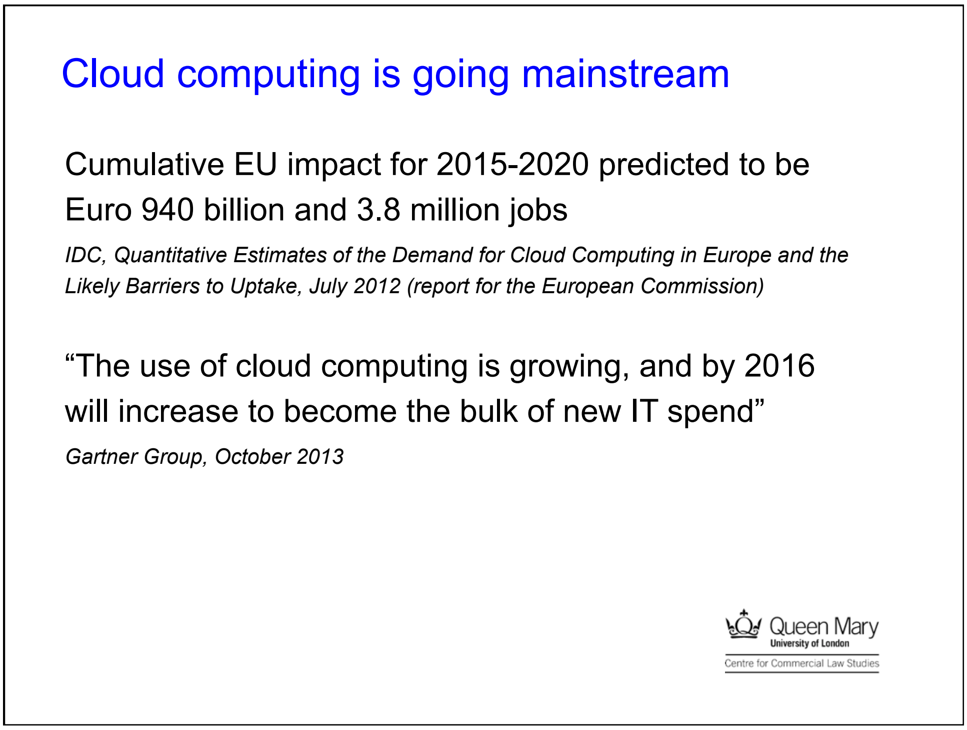
6th November 2014

Data Protection in the Clouds: What Next for Europe?

Christopher Millard

Professor of Privacy and Information Law
Principal Investigator, Cloud Legal Project, Queen Mary University of London
Of Counsel, Bristows

Norwegian Association for Computers & Law
Norwegian Research Centre for Computers & Law



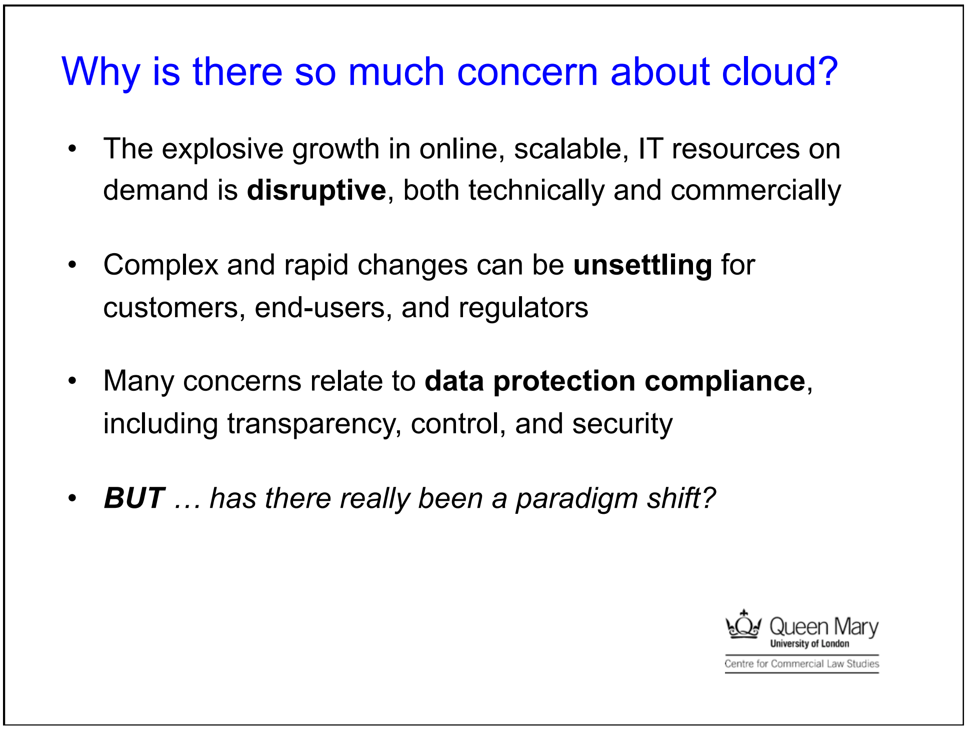
Cloud computing is going mainstream

Cumulative EU impact for 2015-2020 predicted to be Euro 940 billion and 3.8 million jobs

IDC, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake, July 2012 (report for the European Commission)

“The use of cloud computing is growing, and by 2016 will increase to become the bulk of new IT spend”

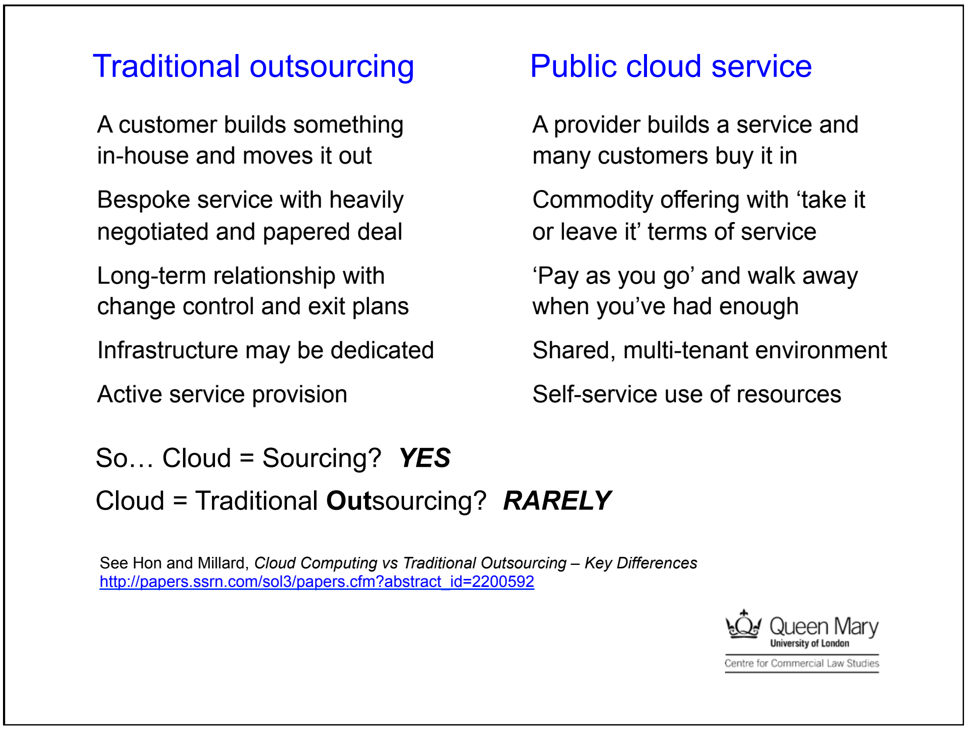
Gartner Group, October 2013



Why is there so much concern about cloud?

- The explosive growth in online, scalable, IT resources on demand is **disruptive**, both technically and commercially
- Complex and rapid changes can be **unsettling** for customers, end-users, and regulators
- Many concerns relate to **data protection compliance**, including transparency, control, and security
- ***BUT*** *… has there really been a paradigm shift?*

Queen Mary University of London Centre for Commercial Law Studies



Traditional outsourcing	Public cloud service
A customer builds something in-house and moves it out	A provider builds a service and many customers buy it in
Bespoke service with heavily negotiated and papered deal	Commodity offering with ‘take it or leave it’ terms of service
Long-term relationship with change control and exit plans	‘Pay as you go’ and walk away when you’ve had enough
Infrastructure may be dedicated	Shared, multi-tenant environment
Active service provision	Self-service use of resources

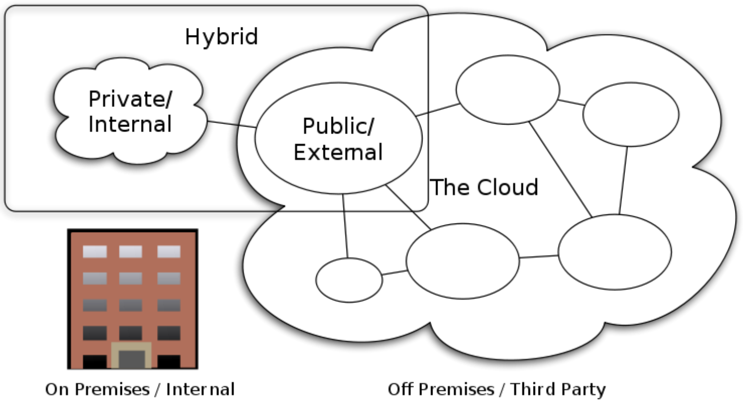
So… Cloud = Sourcing? ***YES***

Cloud = Traditional **Out**sourcing? ***RARELY***

See Hon and Millard, *Cloud Computing vs Traditional Outsourcing – Key Differences* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200592

Queen Mary University of London Centre for Commercial Law Studies

But cloud is not just one thing…



Cloud Computing Types

CC-BY-SA 3.0 by Sam Johnston

Queen Mary University of London
Centre for Commercial Law Studies

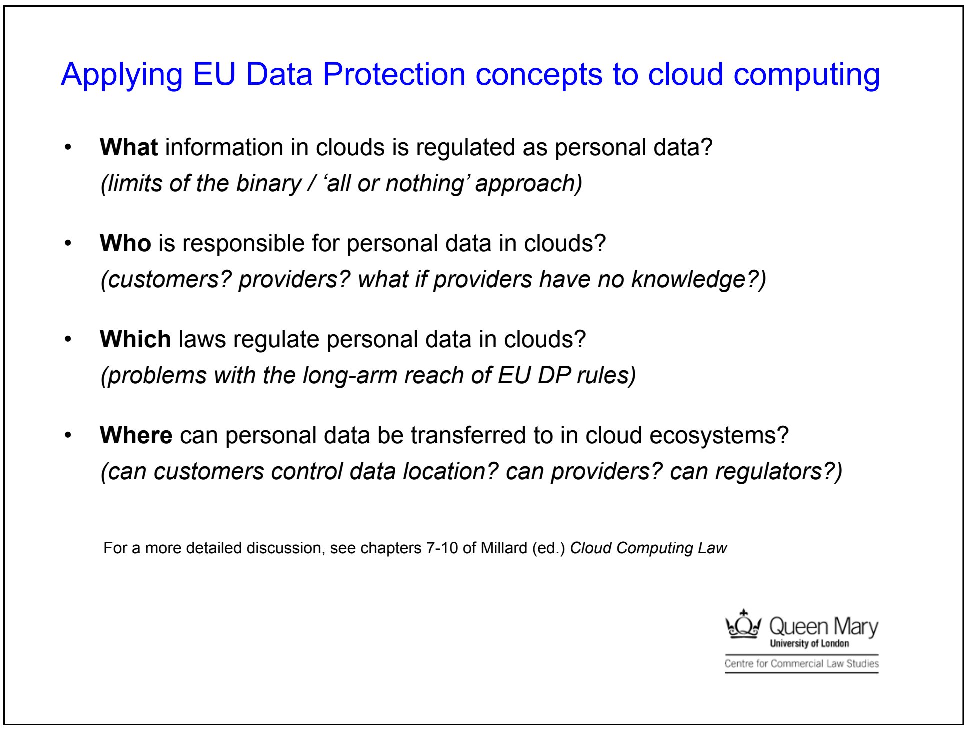
Fastest growing deployment model = hybrid

2013	**2018**
Public = 39%	Hybrid = 43%
Private = 34%	Public = 32%
Hybrid = 27%	Private = 25%

Source: North Bridge - Future of Cloud Computing Survey 2013

Hybrid arrangements tend to be more complex and are more likely to be negotiated

Queen Mary University of London
Centre for Commercial Law Studies

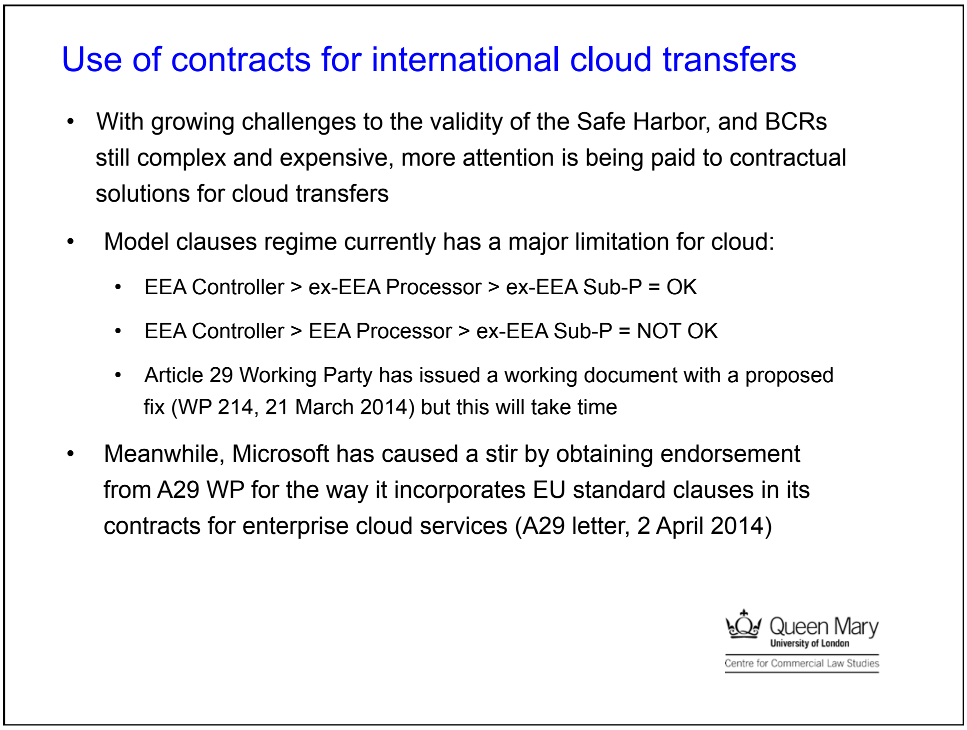


Applying EU Data Protection concepts to cloud computing

- **What** information in clouds is regulated as personal data?
  (limits of the binary / 'all or nothing' approach)
- **Who** is responsible for personal data in clouds?
  (customers? providers? what if providers have no knowledge?)
- **Which** laws regulate personal data in clouds?
  (problems with the long-arm reach of EU DP rules)
- **Where** can personal data be transferred to in cloud ecosystems?
  (can customers control data location? can providers? can regulators?)

For a more detailed discussion, see chapters 7-10 of Millard (ed.) *Cloud Computing Law*

Queen Mary University of London
Centre for Commercial Law Studies



Use of contracts for international cloud transfers

- With growing challenges to the validity of the Safe Harbor, and BCRs still complex and expensive, more attention is being paid to contractual solutions for cloud transfers
- Model clauses regime currently has a major limitation for cloud:
  - EEA Controller > ex-EEA Processor > ex-EEA Sub-P = OK
  - EEA Controller > EEA Processor > ex-EEA Sub-P = NOT OK
  - Article 29 Working Party has issued a working document with a proposed fix (WP 214, 21 March 2014) but this will take time
- Meanwhile, Microsoft has caused a stir by obtaining endorsement from A29 WP for the way it incorporates EU standard clauses in its contracts for enterprise cloud services (A29 letter, 2 April 2014)

Queen Mary University of London
Centre for Commercial Law Studies

Can you control the location of your data in clouds?

- **It depends!**
- Some service providers can't, for technical reasons, or won't, for commercial reasons, let you choose
- Other service providers are designing their clouds so as to offer customers a choice between regions
- Geolocation can be a critical issue for customers that are concerned about where their data are stored because of:
  - Sector-specific compliance requirements (eg. financial services)
  - Restrictions on data transfers (albeit that these are widely ignored)
  - Concerns about disclosure risks associated with litigation / requests from Law Enforcement Authorities - eg. 2014 SDNY 1st instance decision re US access to webmail stored in Dublin (April) + removal of stay (August) + Microsoft declining to comply (September)

Queen Mary University of London
Centre for Commercial Law Studies

What do cloud providers say? - Amazon

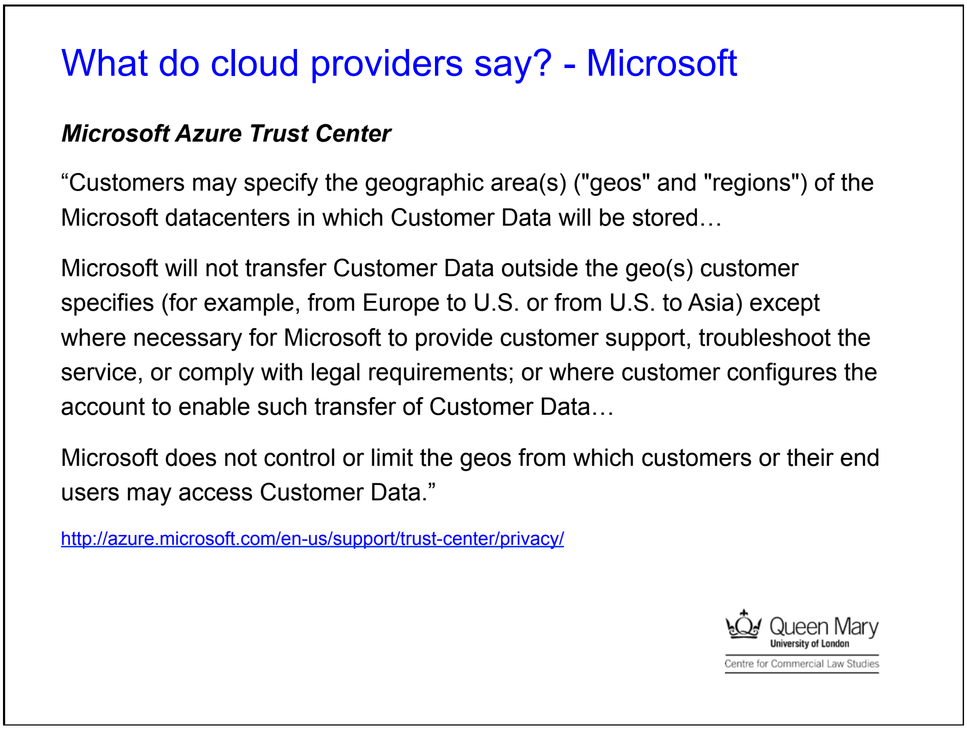
"23 October 2014

Dear AWS Customer,

We are excited to announce the immediate availability of our new EU (Frankfurt) infrastructure region. The Frankfurt region joins Ireland as AWS' second European location, and provides you with a new option for end users and applications benefiting from infrastructure located in continental Europe.

In our new German region, as with all AWS regions, you choose where your data is processed and stored. Additionally, you can now further improve the fault tolerance of your applications using two infrastructure regions located exclusively in Europe…"

Queen Mary University of London
Centre for Commercial Law Studies



What do cloud providers say? - Microsoft

Microsoft Azure Trust Center

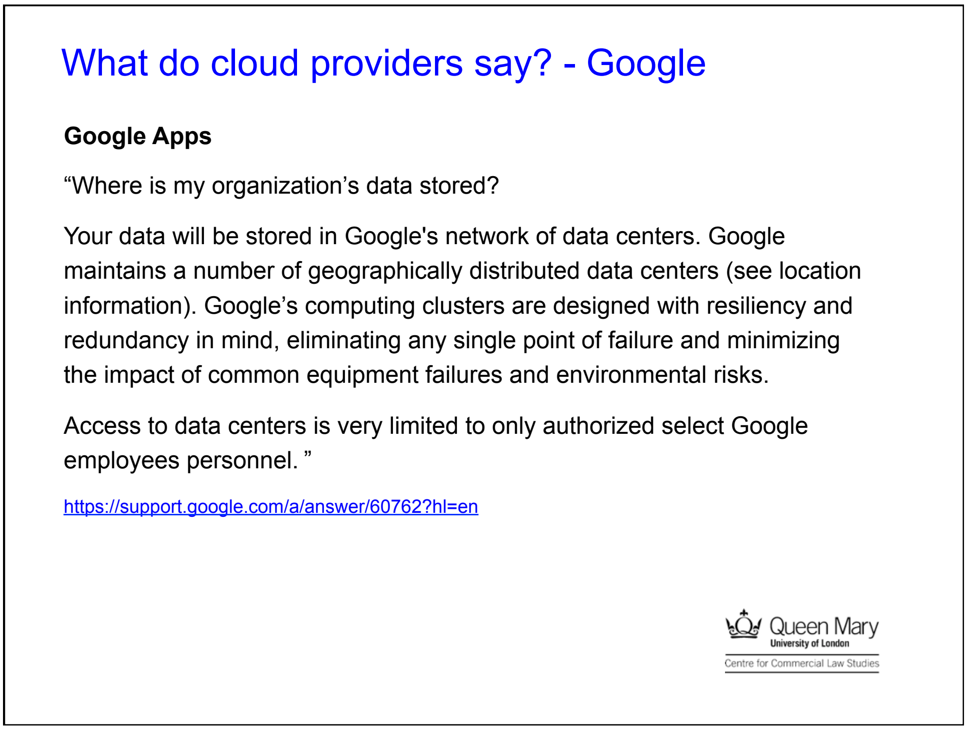
“Customers may specify the geographic area(s) ("geos" and "regions") of the Microsoft datacenters in which Customer Data will be stored…

Microsoft will not transfer Customer Data outside the geo(s) customer specifies (for example, from Europe to U.S. or from U.S. to Asia) except where necessary for Microsoft to provide customer support, troubleshoot the service, or comply with legal requirements; or where customer configures the account to enable such transfer of Customer Data…

Microsoft does not control or limit the geos from which customers or their end users may access Customer Data.”

http://azure.microsoft.com/en-us/support/trust-center/privacy/

Queen Mary
University of London
Centre for Commercial Law Studies



What do cloud providers say? - Google

Google Apps

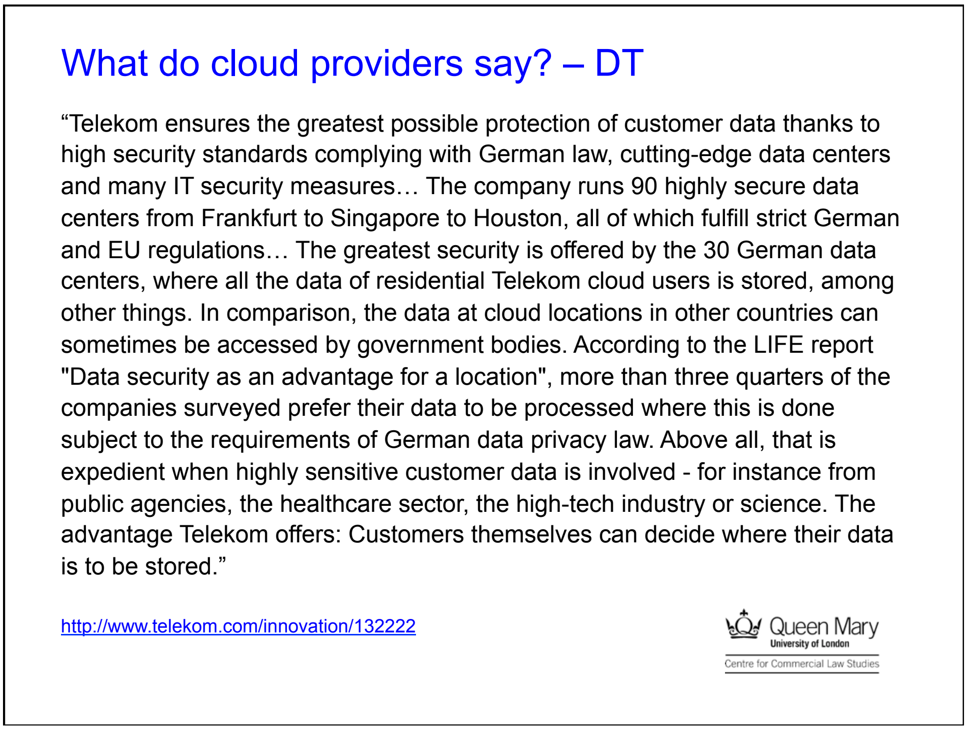
“Where is my organization’s data stored?

Your data will be stored in Google's network of data centers. Google maintains a number of geographically distributed data centers (see location information). Google’s computing clusters are designed with resiliency and redundancy in mind, eliminating any single point of failure and minimizing the impact of common equipment failures and environmental risks.

Access to data centers is very limited to only authorized select Google employees personnel. ”

https://support.google.com/a/answer/60762?hl=en

Queen Mary
University of London
Centre for Commercial Law Studies

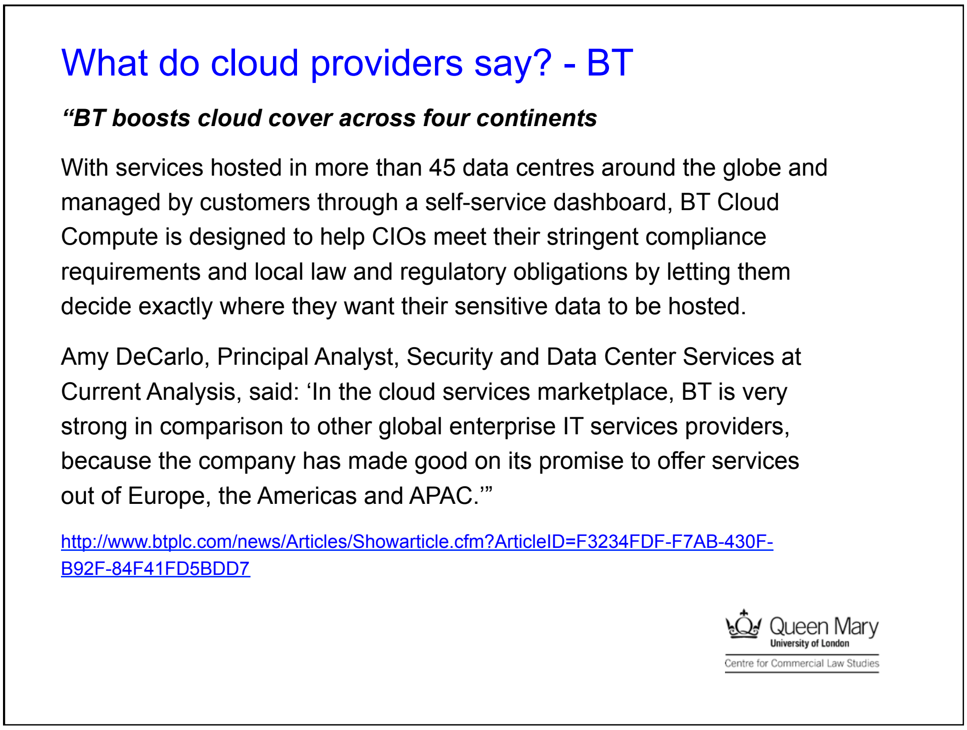


What do cloud providers say? – DT

“Telekom ensures the greatest possible protection of customer data thanks to high security standards complying with German law, cutting-edge data centers and many IT security measures… The company runs 90 highly secure data centers from Frankfurt to Singapore to Houston, all of which fulfill strict German and EU regulations… The greatest security is offered by the 30 German data centers, where all the data of residential Telekom cloud users is stored, among other things. In comparison, the data at cloud locations in other countries can sometimes be accessed by government bodies. According to the LIFE report "Data security as an advantage for a location", more than three quarters of the companies surveyed prefer their data to be processed where this is done subject to the requirements of German data privacy law. Above all, that is expedient when highly sensitive customer data is involved - for instance from public agencies, the healthcare sector, the high-tech industry or science. The advantage Telekom offers: Customers themselves can decide where their data is to be stored.”

http://www.telekom.com/innovation/132222

Queen Mary
University of London
Centre for Commercial Law Studies



What do cloud providers say? - BT

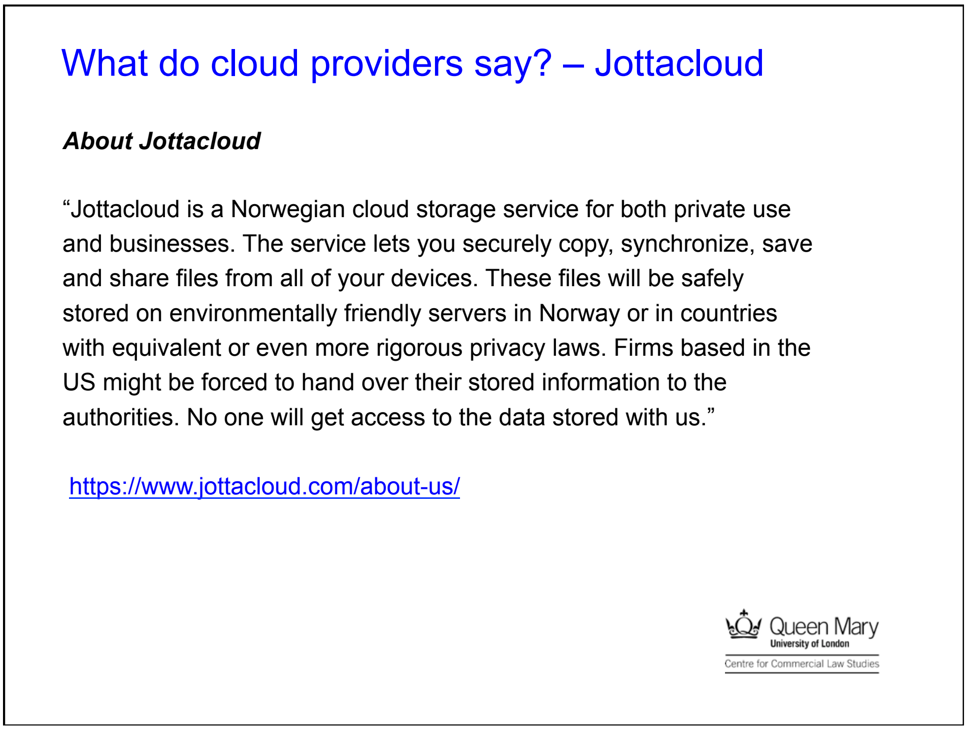
“BT boosts cloud cover across four continents

With services hosted in more than 45 data centres around the globe and managed by customers through a self-service dashboard, BT Cloud Compute is designed to help CIOs meet their stringent compliance requirements and local law and regulatory obligations by letting them decide exactly where they want their sensitive data to be hosted.

Amy DeCarlo, Principal Analyst, Security and Data Center Services at Current Analysis, said: ‘In the cloud services marketplace, BT is very strong in comparison to other global enterprise IT services providers, because the company has made good on its promise to offer services out of Europe, the Americas and APAC.’”

http://www.btplc.com/news/Articles/Showarticle.cfm?ArticleID=F3234FDF-F7AB-430F-B92F-84F41FD5BDD7

Queen Mary
University of London
Centre for Commercial Law Studies



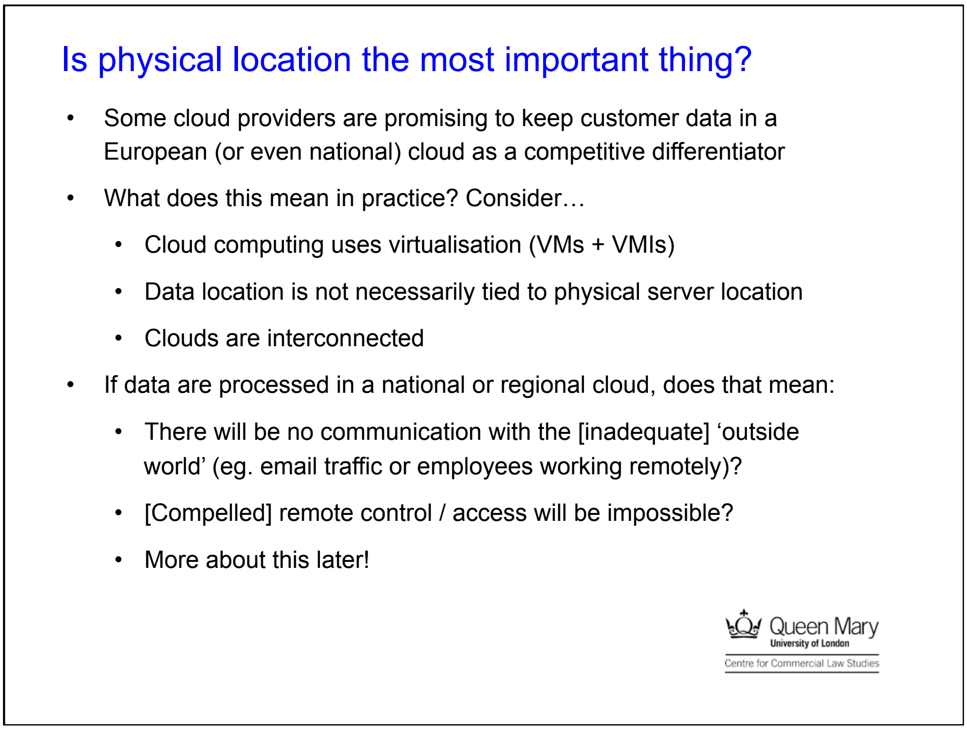
What do cloud providers say? – Jottacloud

About Jottacloud

“Jottacloud is a Norwegian cloud storage service for both private use and businesses. The service lets you securely copy, synchronize, save and share files from all of your devices. These files will be safely stored on environmentally friendly servers in Norway or in countries with equivalent or even more rigorous privacy laws. Firms based in the US might be forced to hand over their stored information to the authorities. No one will get access to the data stored with us.”

https://www.jottacloud.com/about-us/

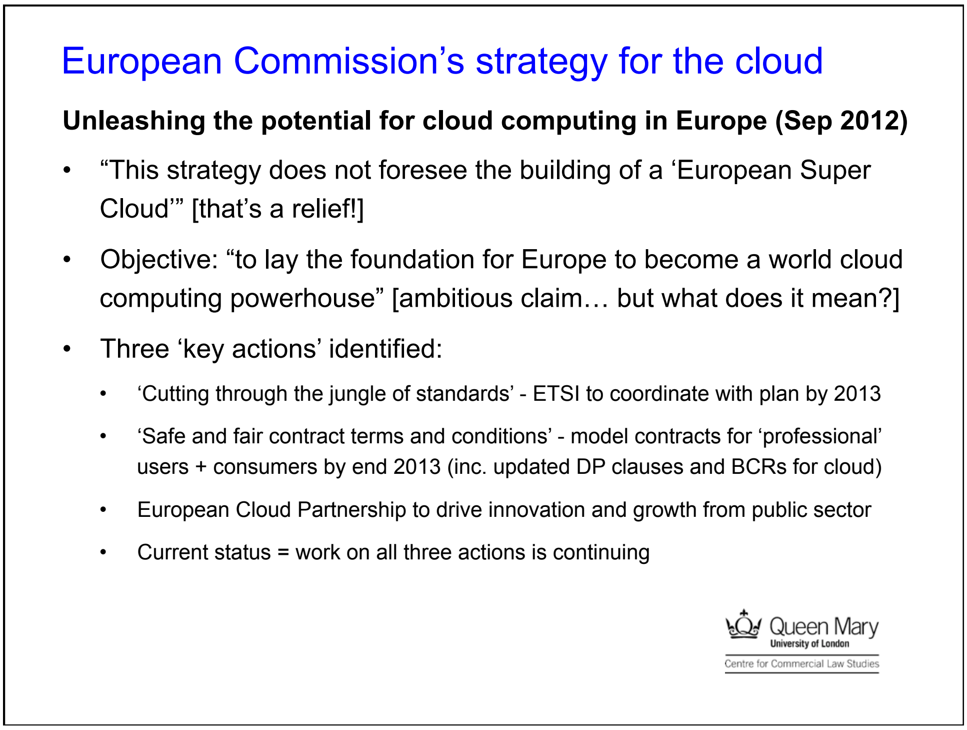
Queen Mary
University of London
Centre for Commercial Law Studies



Is physical location the most important thing?

- Some cloud providers are promising to keep customer data in a European (or even national) cloud as a competitive differentiator
- What does this mean in practice? Consider…
  - Cloud computing uses virtualisation (VMs + VMIs)
  - Data location is not necessarily tied to physical server location
  - Clouds are interconnected
- If data are processed in a national or regional cloud, does that mean:
  - There will be no communication with the [inadequate] ‘outside world’ (eg. email traffic or employees working remotely)?
  - [Compelled] remote control / access will be impossible?
  - More about this later!

Queen Mary
University of London
Centre for Commercial Law Studies

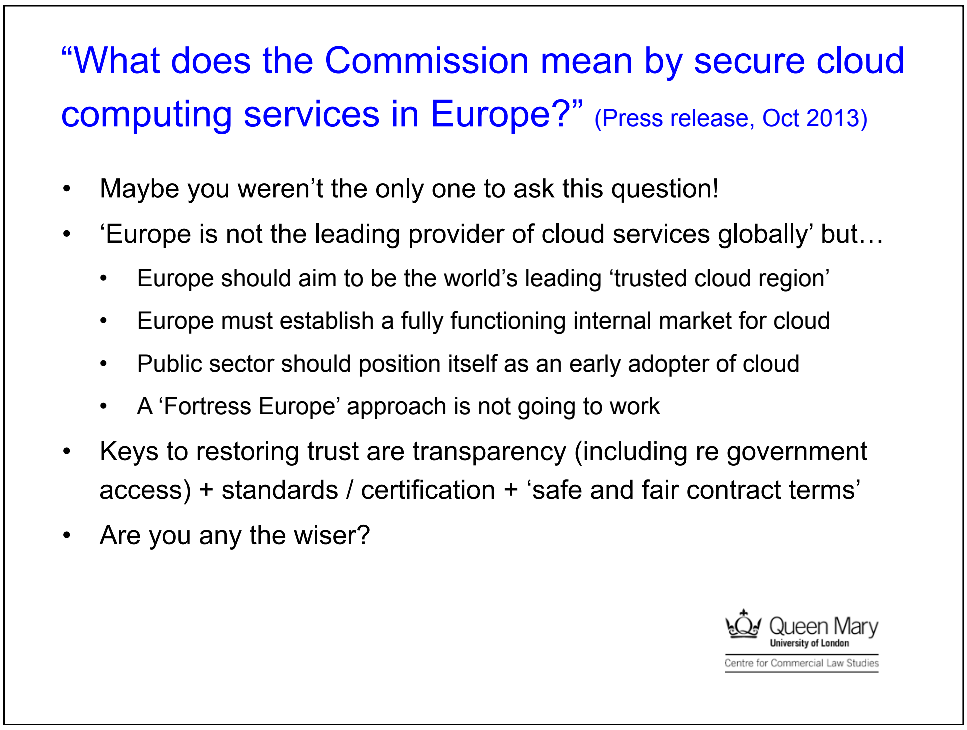


European Commission’s strategy for the cloud

Unleashing the potential for cloud computing in Europe (Sep 2012)

- “This strategy does not foresee the building of a ‘European Super Cloud’” [that’s a relief!]
- Objective: “to lay the foundation for Europe to become a world cloud computing powerhouse” [ambitious claim… but what does it mean?]
- Three ‘key actions’ identified:
  - ‘Cutting through the jungle of standards’ - ETSI to coordinate with plan by 2013
  - ‘Safe and fair contract terms and conditions’ - model contracts for ‘professional’ users + consumers by end 2013 (inc. updated DP clauses and BCRs for cloud)
  - European Cloud Partnership to drive innovation and growth from public sector
  - Current status = work on all three actions is continuing

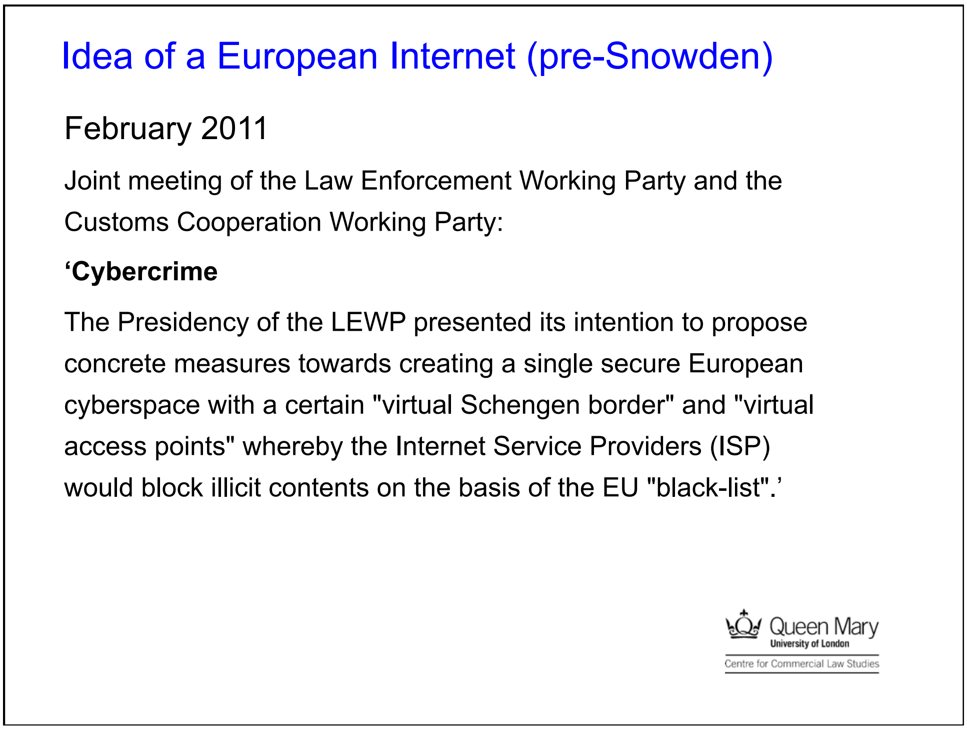
Queen Mary University of London
Centre for Commercial Law Studies



“What does the Commission mean by secure cloud computing services in Europe?” (Press release, Oct 2013)

- Maybe you weren’t the only one to ask this question!
- ‘Europe is not the leading provider of cloud services globally’ but…
  - Europe should aim to be the world’s leading ‘trusted cloud region’
  - Europe must establish a fully functioning internal market for cloud
  - Public sector should position itself as an early adopter of cloud
  - A ‘Fortress Europe’ approach is not going to work
- Keys to restoring trust are transparency (including re government access) + standards / certification + ‘safe and fair contract terms’
- Are you any the wiser?

Queen Mary University of London
Centre for Commercial Law Studies



Idea of a European Internet (pre-Snowden)

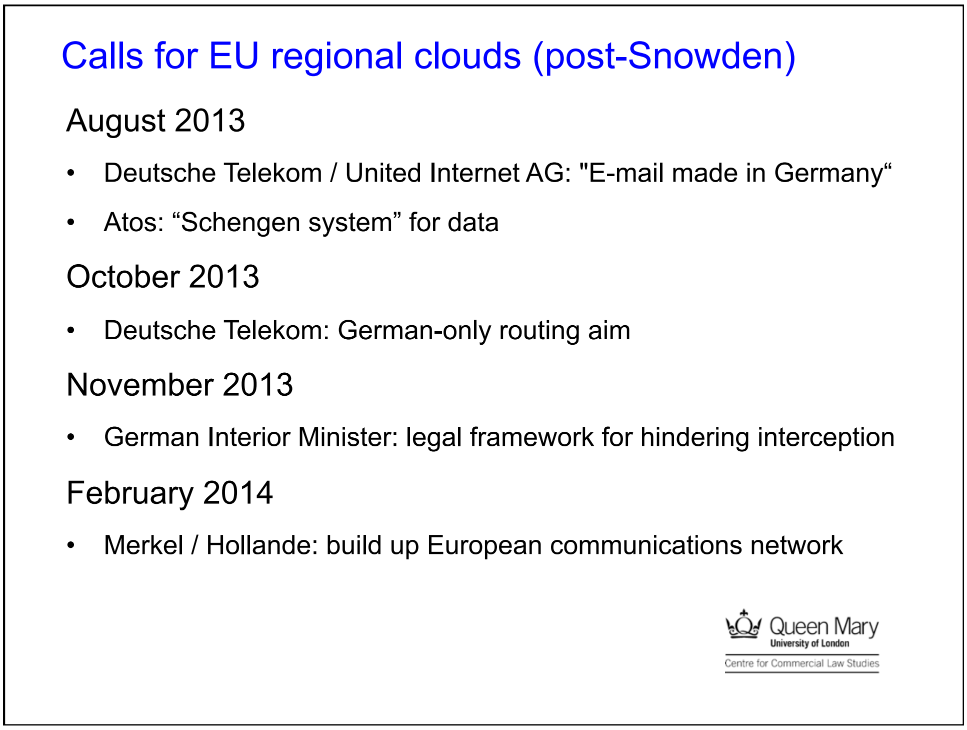
February 2011

Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party:

‘Cybercrime

The Presidency of the LEWP presented its intention to propose concrete measures towards creating a single secure European cyberspace with a certain "virtual Schengen border" and "virtual access points" whereby the Internet Service Providers (ISP) would block illicit contents on the basis of the EU "black-list".’

Queen Mary
University of London
Centre for Commercial Law Studies



Calls for EU regional clouds (post-Snowden)

August 2013

- Deutsche Telekom / United Internet AG: "E-mail made in Germany“
- Atos: “Schengen system” for data

October 2013

- Deutsche Telekom: German-only routing aim

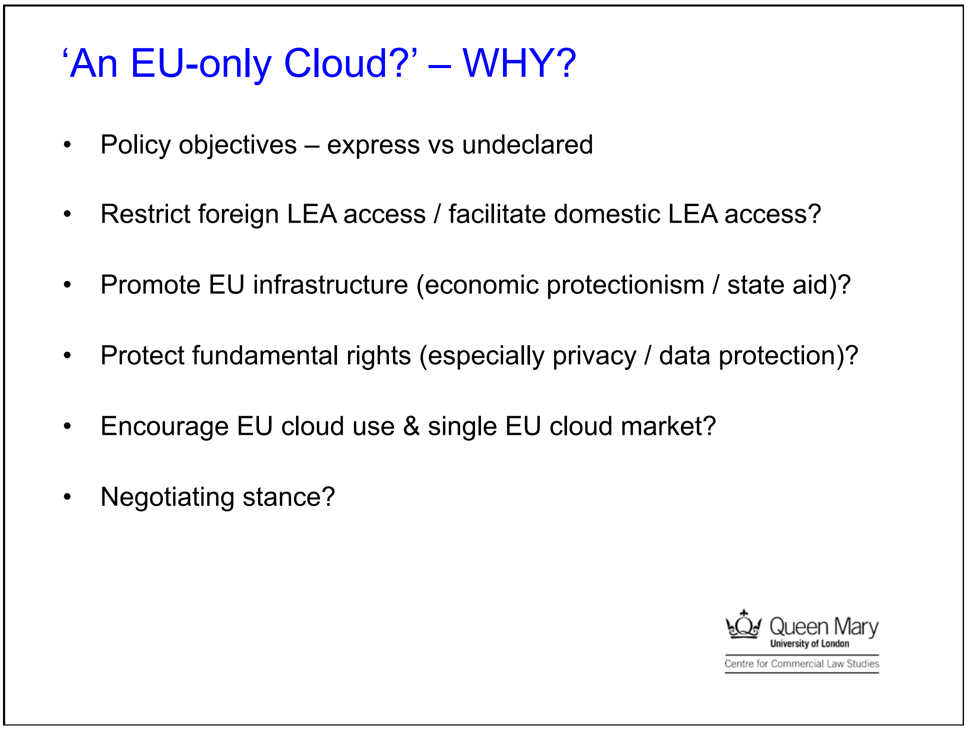
November 2013

- German Interior Minister: legal framework for hindering interception

February 2014

- Merkel / Hollande: build up European communications network

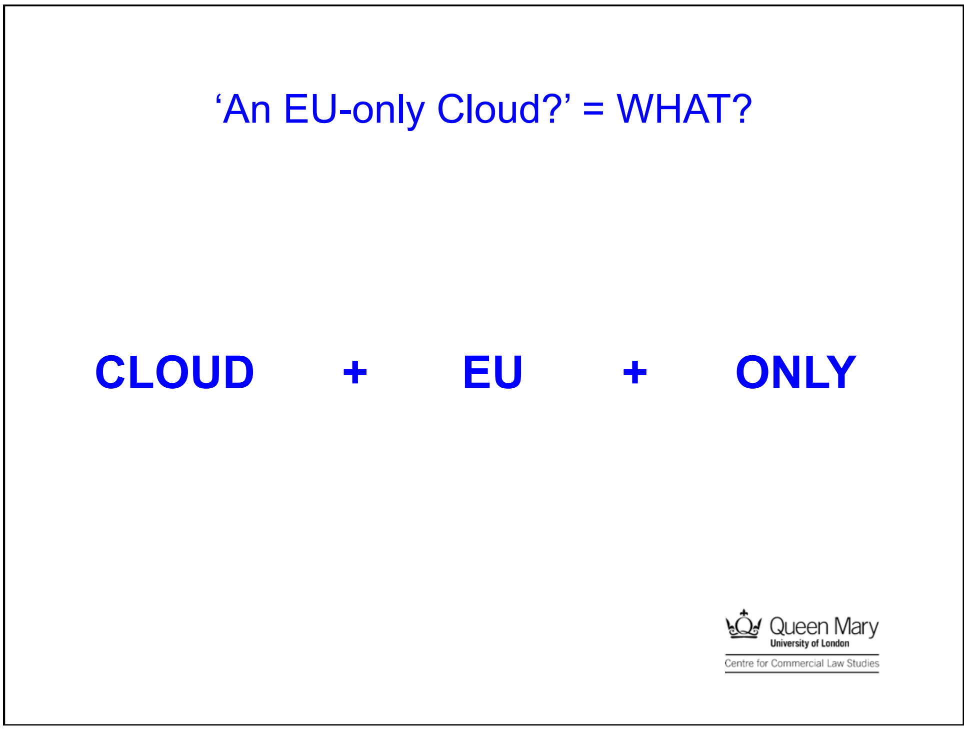
Queen Mary
University of London
Centre for Commercial Law Studies



‘An EU-only Cloud?’ – WHY?

- Policy objectives – express vs undeclared
- Restrict foreign LEA access / facilitate domestic LEA access?
- Promote EU infrastructure (economic protectionism / state aid)?
- Protect fundamental rights (especially privacy / data protection)?
- Encourage EU cloud use & single EU cloud market?
- Negotiating stance?

Queen Mary University of London
Centre for Commercial Law Studies

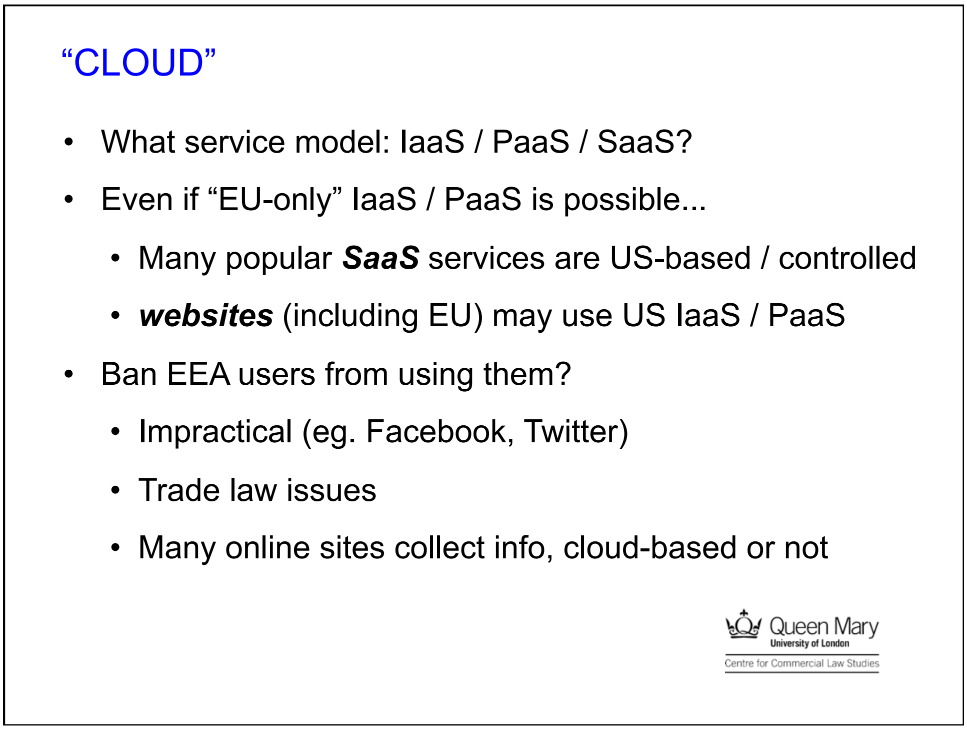


‘An EU-only Cloud?’ = WHAT?

CLOUD + EU + ONLY

Queen Mary University of London
Centre for Commercial Law Studies

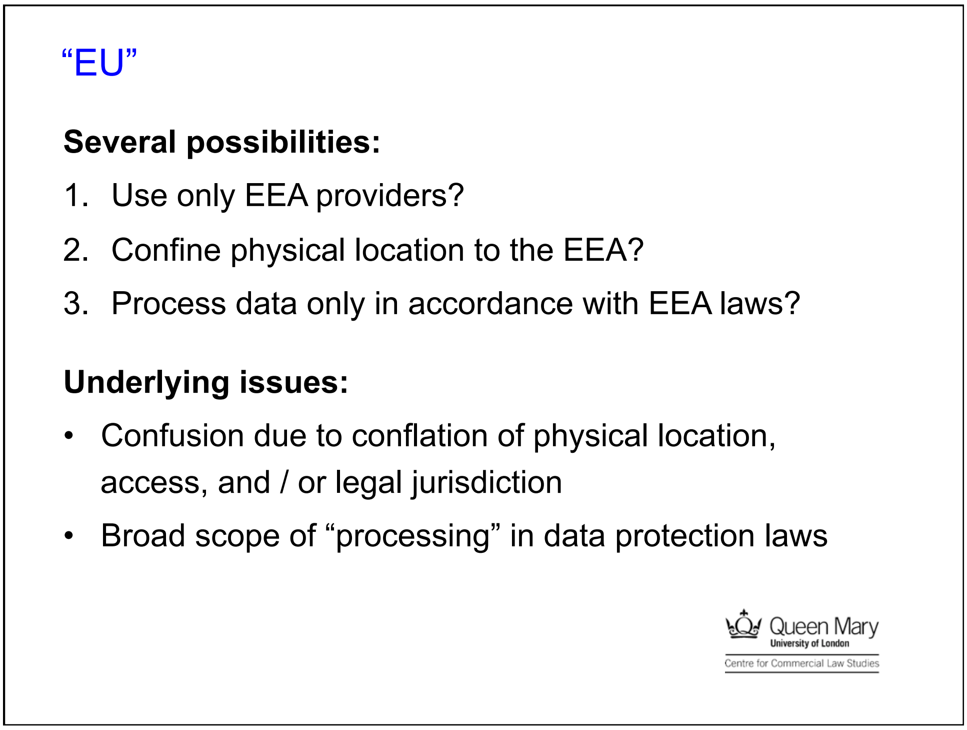
“Cloud”



“CLOUD”

- What service model: IaaS / PaaS / SaaS?
- Even if “EU-only” IaaS / PaaS is possible...
  - Many popular ***SaaS*** services are US-based / controlled
  - ***websites*** (including EU) may use US IaaS / PaaS
- Ban EEA users from using them?
  - Impractical (eg. Facebook, Twitter)
  - Trade law issues
  - Many online sites collect info, cloud-based or not

“EU”



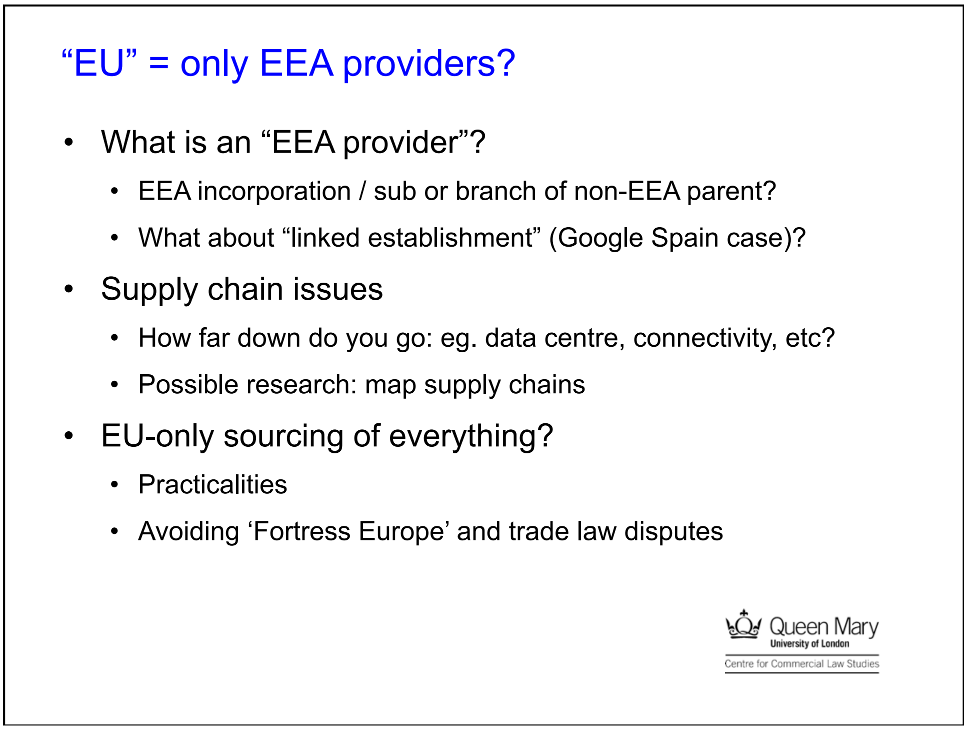
“EU”

Several possibilities:

1. Use only EEA providers?
2. Confine physical location to the EEA?
3. Process data only in accordance with EEA laws?

Underlying issues:

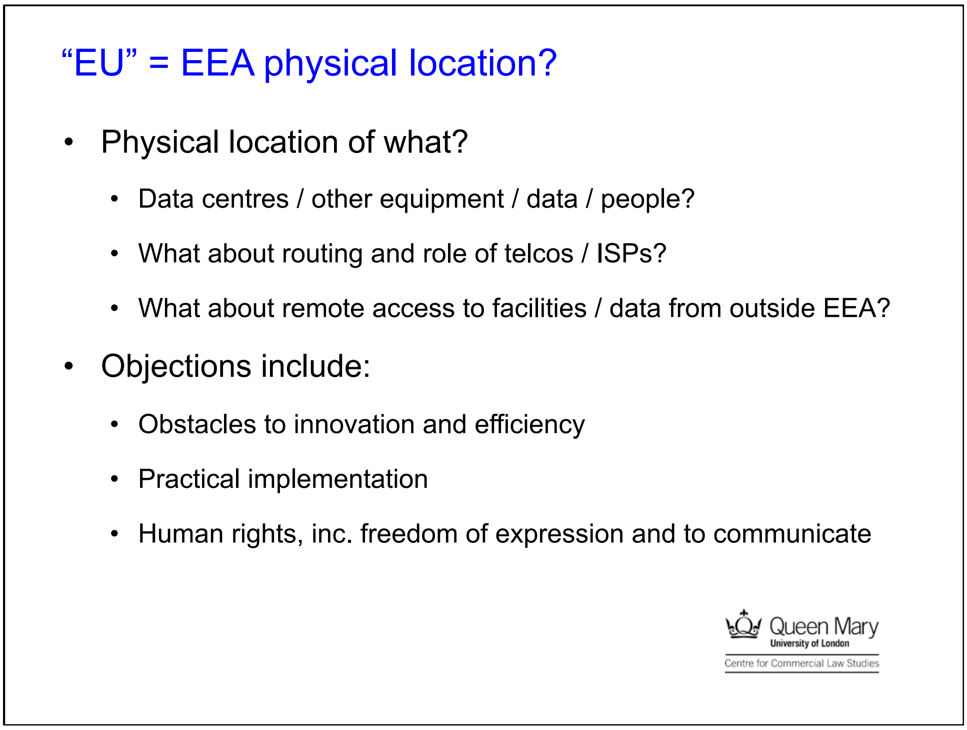
- Confusion due to conflation of physical location, access, and / or legal jurisdiction
- Broad scope of “processing” in data protection laws



“EU” = only EEA providers?

- What is an “EEA provider”?
  - EEA incorporation / sub or branch of non-EEA parent?
  - What about “linked establishment” (Google Spain case)?
- Supply chain issues
  - How far down do you go: eg. data centre, connectivity, etc?
  - Possible research: map supply chains
- EU-only sourcing of everything?
  - Practicalities
  - Avoiding ‘Fortress Europe’ and trade law disputes

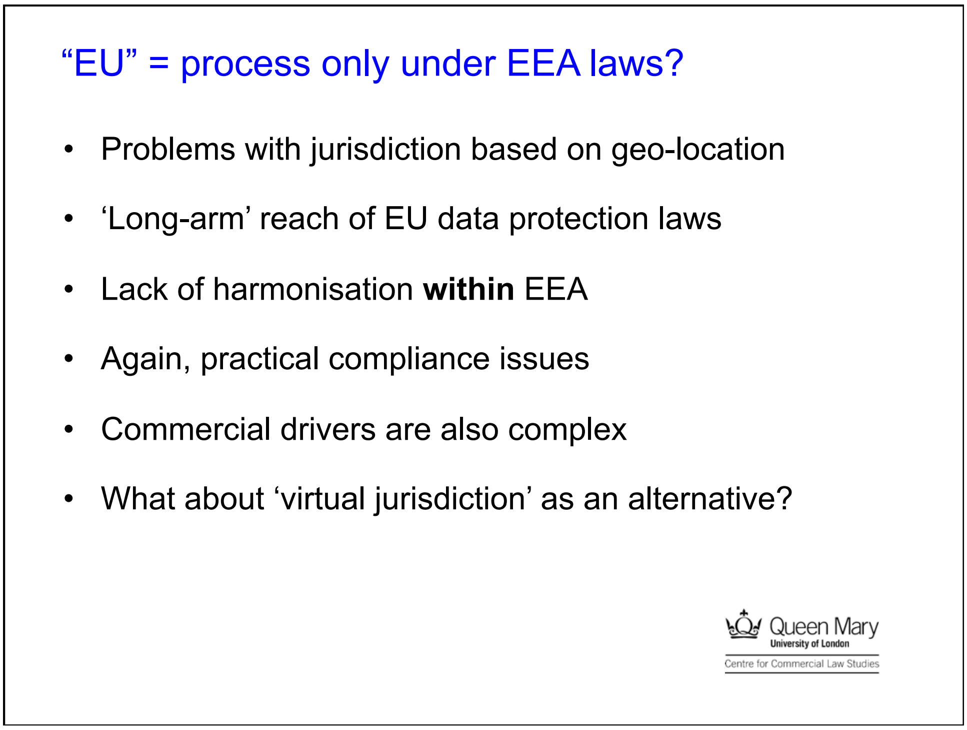
Queen Mary
University of London
Centre for Commercial Law Studies



“EU” = EEA physical location?

- Physical location of what?
  - Data centres / other equipment / data / people?
  - What about routing and role of telcos / ISPs?
  - What about remote access to facilities / data from outside EEA?
- Objections include:
  - Obstacles to innovation and efficiency
  - Practical implementation
  - Human rights, inc. freedom of expression and to communicate

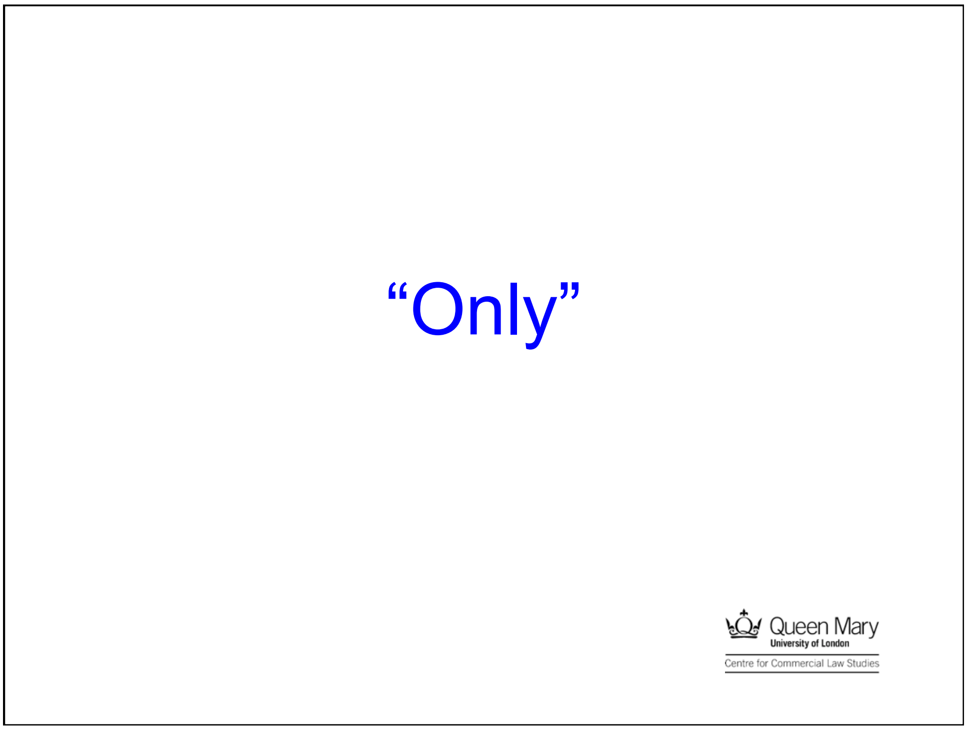
Queen Mary
University of London
Centre for Commercial Law Studies



“EU” = process only under EEA laws?

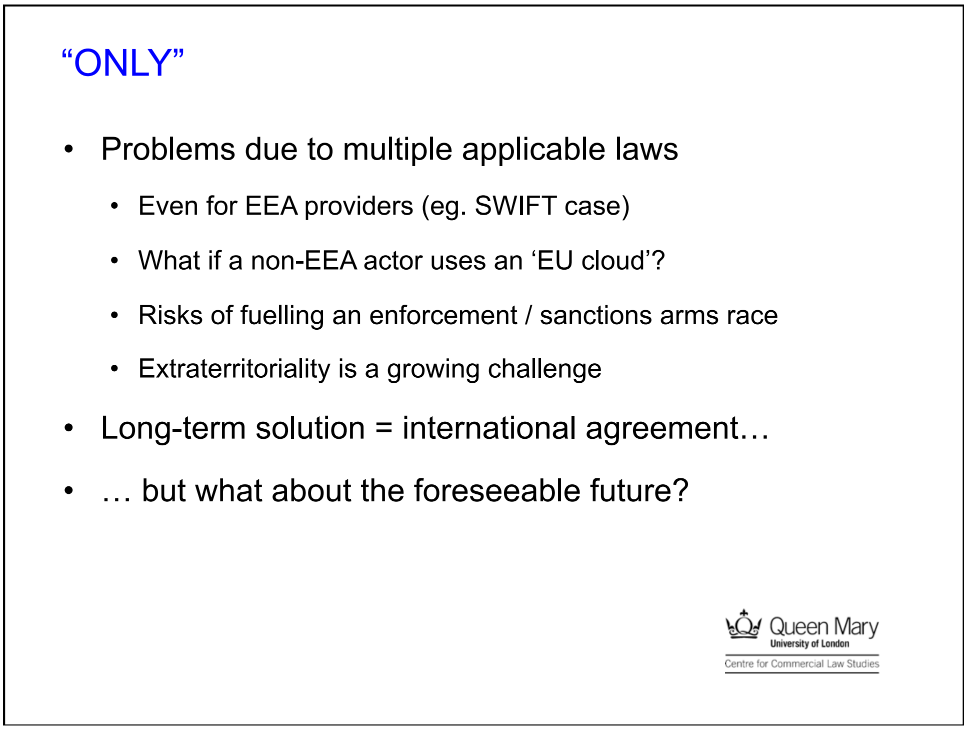
- Problems with jurisdiction based on geo-location
- ‘Long-arm’ reach of EU data protection laws
- Lack of harmonisation **within** EEA
- Again, practical compliance issues
- Commercial drivers are also complex
- What about ‘virtual jurisdiction’ as an alternative?

Queen Mary University of London
Centre for Commercial Law Studies



“Only”

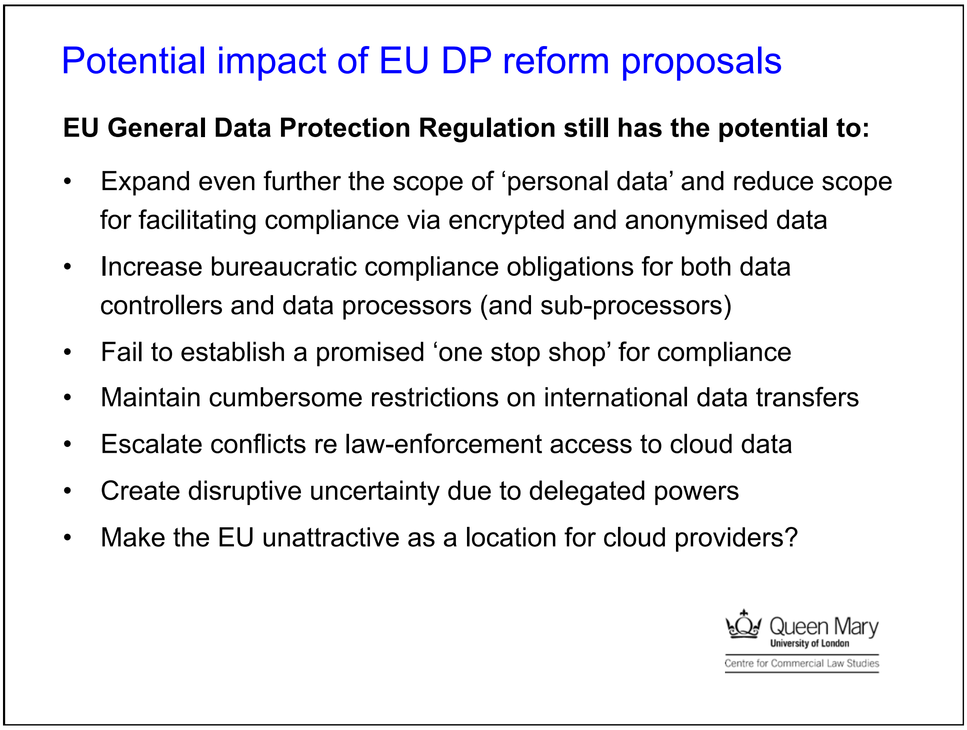
Queen Mary University of London
Centre for Commercial Law Studies



“ONLY”

- Problems due to multiple applicable laws
  - Even for EEA providers (eg. SWIFT case)
  - What if a non-EEA actor uses an ‘EU cloud’?
  - Risks of fuelling an enforcement / sanctions arms race
  - Extraterritoriality is a growing challenge
- Long-term solution = international agreement…
- … but what about the foreseeable future?

Queen Mary
University of London
Centre for Commercial Law Studies



Potential impact of EU DP reform proposals

EU General Data Protection Regulation still has the potential to:

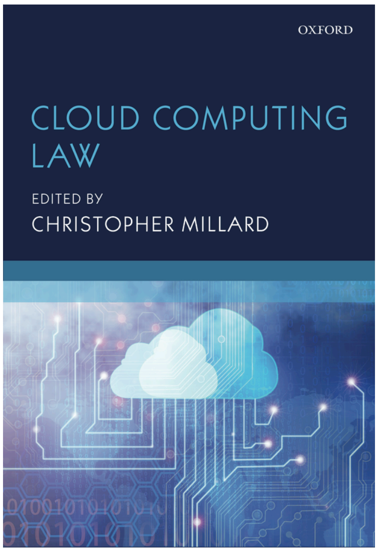
- Expand even further the scope of ‘personal data’ and reduce scope for facilitating compliance via encrypted and anonymised data
- Increase bureaucratic compliance obligations for both data controllers and data processors (and sub-processors)
- Fail to establish a promised ‘one stop shop’ for compliance
- Maintain cumbersome restrictions on international data transfers
- Escalate conflicts re law-enforcement access to cloud data
- Create disruptive uncertainty due to delegated powers
- Make the EU unattractive as a location for cloud providers?

Queen Mary
University of London
Centre for Commercial Law Studies

And finally…

I still don't know when you will be able to see the movie…

… but you can buy the book from Amazon now!



OXFORD

CLOUD COMPUTING LAW

EDITED BY
CHRISTOPHER MILLARD

Queen Mary
University of London
Centre for Commercial Law Studies

Thanks for listening!

Any questions…

You may find some answers here:
http://www.cloudlegal.ccls.qmul.ac.uk/

Queen Mary
University of London
Centre for Commercial Law Studies