CILP, University of Toronto

14th October 2011

The What, Who and Where of Cloud Privacy: a European Perspective

Professor Christopher Millard

Centre for Commercial Law Studies, Queen Mary, University of London

www.cloudlegal.ccls.qmul.ac.uk / c.millard@qmul.ac.uk

Queen Mary University of London

Centre for Commercial Law Studies

Some privacy questions we will tackle today…

- **What** information in clouds is regulated as ‘personal data’?
- **Who** is responsible for personal data in clouds?
- **Where** do data protection laws reach to in clouds?
- **What** do cloud contracts typically say about personal data?

But first…

- **What** do we mean by ‘cloud computing’? *and*
- **Why** is it such a hot topic?

Queen Mary
University of London
Centre for Commercial Law Studies

What is cloud computing?

- It usually involves the provision of scalable IT resources (data storage, application hosting, *etc.*) on demand, delivered via the Internet
- Many concepts and definitions but a common starting point is often this definition from the Gartner Group:

  "A style of computing where scalable and elastic IT capabilities are provided as a service to multiple customers using Internet technologies"
- Prominent examples include:
  - Amazon Web Services
  - Gmail and GoogleApps
  - Microsoft Hotmail + Office 365 + Windows Azure
  - IBM Smart Business + CloudBurst (previously Blue Cloud)
  - Safesforce.com
  - AND …Facebook, Apple, PayPal and other cloud app platform providers

Why is cloud computing such a hot topic?

- Various factors are transforming remote computing, including high-bandwidth low-cost connectivity, development of large server farms and enabling techniques such as virtualisation and sharding
- In the current economic climate, cloud computing may be attractive as a means of:
  - achieving rapid outsourcing efficiencies
  - cost reduction / converting capex to opex
  - simplifying hardware and software maintenance
  - smoothing fluctuations in demand levels
  - delivering public sector services more efficiently, see *eg.*
    - In the UK - *Digital Britain* and the *G-Cloud*
    - In the US - *Apps.gov*

GSA Apps.Gov
A Service Provided by GSA

Welcome Register | Log In

0 Items in Cart **$0.00**

Contact Us | Cloud FAQs

Home **Business Apps** **Productivity Apps** **Cloud IT Services** **Social Media Apps**

Sunday, September 20, 2009

SEARCH FOR **IN** All Categories GO

Welcome to Apps.gov

Apps.gov is your source for cloud computing applications designed to help your agency harness the power of today's technology. Whether it's Business or Productivity Applications, Cloud IT Services or Social Media solutions, Apps.gov is the place to get your government agency in the cloud.

What is Cloud Computing?

Want to learn more?

Watch this brief video for an overview of Cloud Computing to gain a better understanding of what it is and its benefits.

Watch the video now »

What type of solution do you need?

Business Apps

Your agency or service is complex and requires state-of-the-art software to get business done.

GSA Cloud Business Apps has a solution!

Cloud IT Services

Need a better solution to reduce cost and implement projects faster?

GSA Cloud IT Services has the answer!

Productivity Apps

You need to get things done and GSA is there to help you do just that.

GSA Cloud Productivity Apps has the tools!

Social Media Apps

Social media tools make it easier to discuss the things we care about and help us get the job done.

GSA Social Media Apps can help you get the word out!

So, everyone must think cloud computing is great!

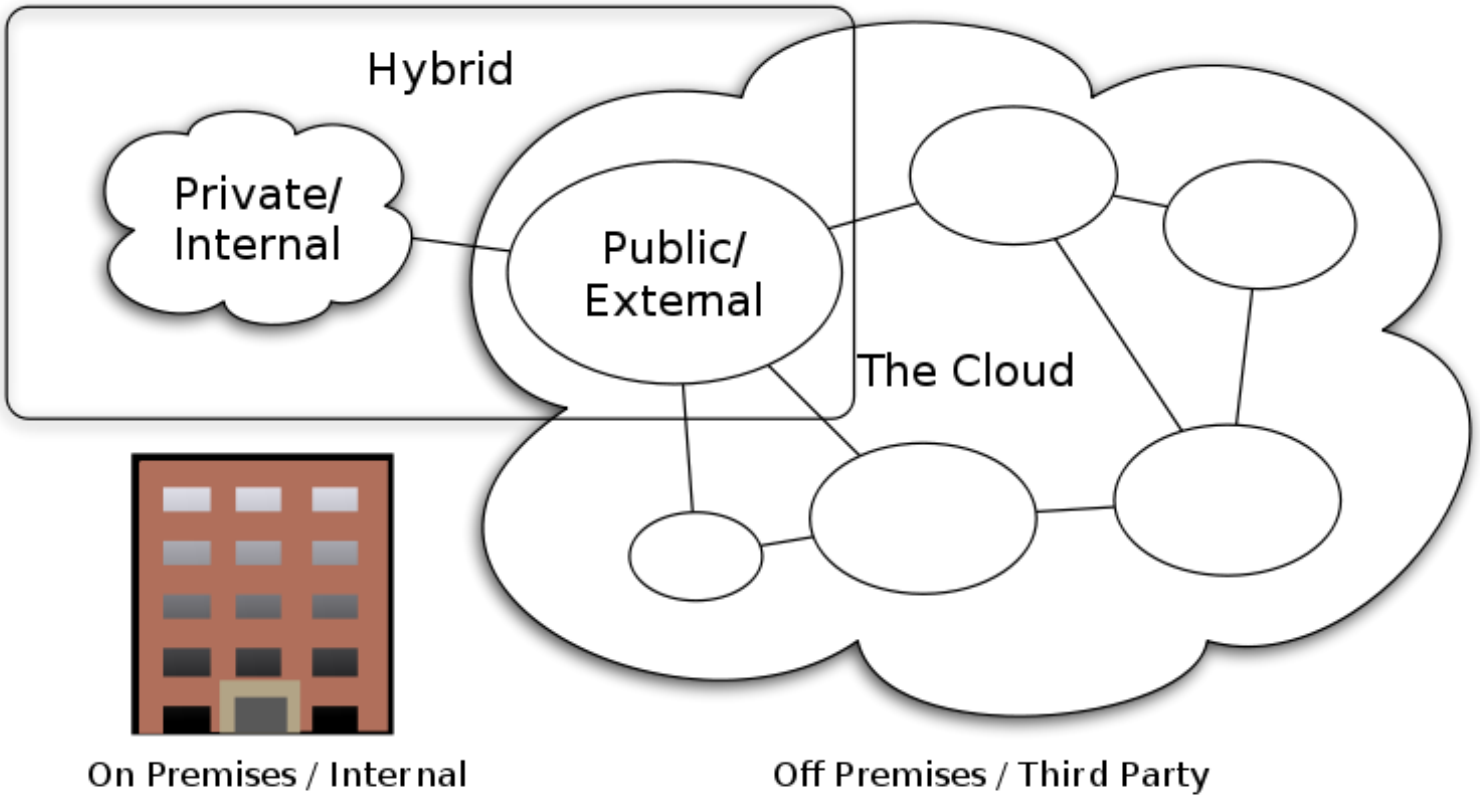
"It's stupidity. Its worse than stupidity: it's a marketing hype campaign"
Richard Stallman (Founder of the Free Software Foundation), September 2008

"If you believe the hype, cloud computing is the future. Hype aside, cloud computing is nothing new."
Bruce Schneier, writing in the Guardian, June 2009

"The rise of the cloud is more than just another platform shift that gets geeks excited. It will undoubtedly transform the information technology industry, but it will also profoundly change the way people work and companies operate. It will allow digital technology to penetrate every nook and cranny of the economy and of society, creating some tricky political problems along the way."
The Economist, October 2008

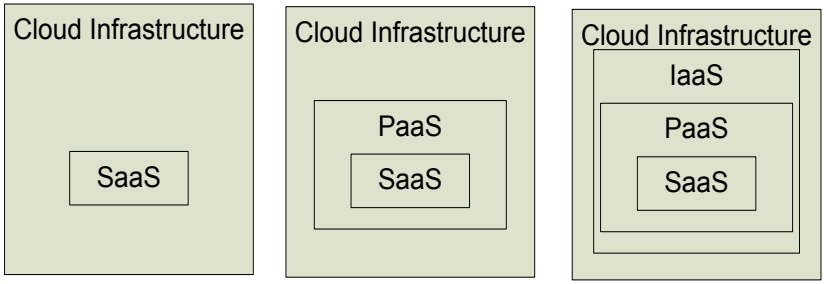
Global market for cloud computing services is predicted to grow from $40.7billion (2011) to $241 billion (2020)
Forrester Research, April 2011

Cloud architectures: the public / private mix …

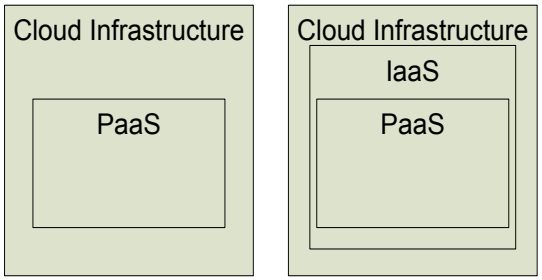


Queen Mary
University of London
Centre for Commercial Law Studies

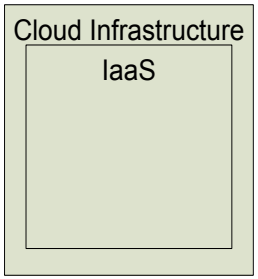
Another way to look at clouds (including hidden layers)



Software as a Service (SaaS) Architectures



Platform as a Service (PaaS) Architectures



Infrastructure as a Service (IaaS) Architectures

From
http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt

Queen Mary
University of London
Centre for Commercial Law Studies

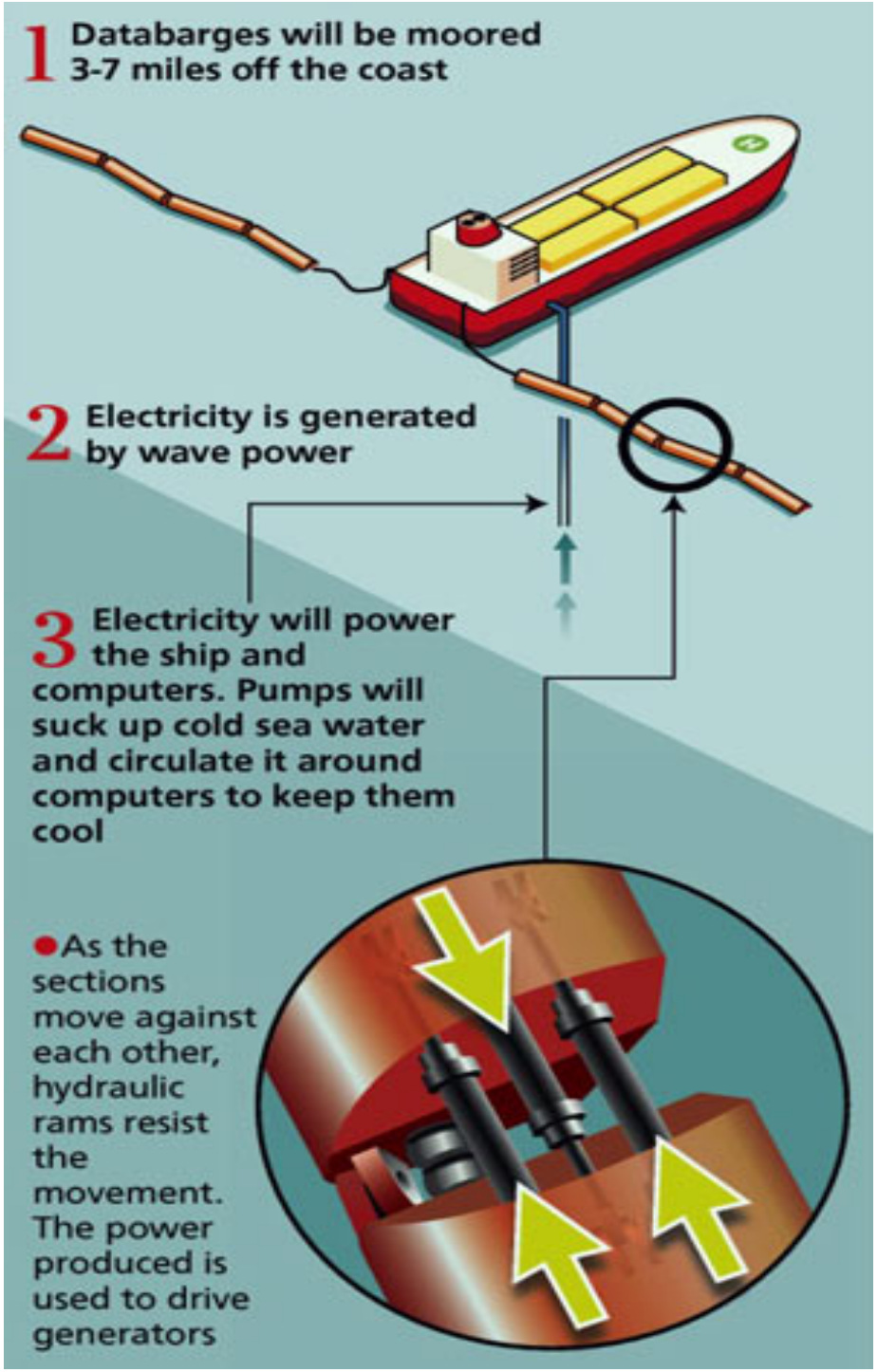
Major cloud players have substantial infrastructure…

- Massive data centres are being built, often containing sealed shipping containers, themselves containing pre-configured servers
- Location remains very important
- Huge requirements for power / cooling / connectivity
- Google has patented a "water-based data center" - a system that includes "a floating platform-mounted computer data center comprising a plurality of computing units, a sea-based electrical generator in electrical connection with the plurality of computing units, and one or more sea-water cooling units for providing cooling to the plurality of computing units."

So just when we thought we had identified all the technical, commercial and legal risks associated with outsourcing and offshore data processing …

…we have to tackle maritime law

…and the risk of meeting real pirates on the high seas!



What is regulated as 'personal data' in clouds?

- Cloud processing arrangements may involve…
  - a spectrum of activities with diverse identification requirements
  - anonymisation / pseudonymisation
  - encryption
  - sharding / virtualisation / distributed storage
- Personal data: limits of the 'all or nothing' / binary approach
- Should risk of identification / risk of harm be factors?

Queen Mary
University of London
Centre for Commercial Law Studies

Who is responsible for personal data in clouds?

- Cloud customers?
- Cloud providers?
  - Customer account data / metadata
  - Personal data processed by customer in the cloud
  - Distinguishing between IaaS, PaaS, SaaS, etc
- Generally assumed that a cloud provider will be…
  - A data controller ***or***
  - A data processor ***or***
  - Both

Queen Mary
University of London
Centre for Commercial Law Studies

What should a cloud provider's status be?

- EU Article 29 Working Party paper on controllers & processors:
  - Cloud computing is further "blurring the distinction between data controllers, processors and data subjects"
  - About factual, functional control not just contracts / labels [*eg.* SWIFT]
  - Cloud providers have some "margin of manoeuvre" in determining "means" of processing: "effective means" may be better test [not clear!]
- What about the possibility that a provider may be **neither** a controller **nor** a processor of customer data in certain circumstances?
- Alternatives include:
  - End to end accountability - *eg* Canadian PIPEDA model
  - eCommerce Directive model - recognise a mere conduit role (not just for telcos but perhaps also to cover some cloud hosting and caching)

Where do European data protection laws reach to (1)?

- If… “processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State” *THEN* national DP law can have global reach, ***but***
  - What constitutes ‘establishment’?
  - What is the status of own and third party cloud data centres in EEA?
- If not established in EEA but use ‘equipment’ / ‘means’ in EEA also regulated and must appoint an agent, ***but***
  - What if EEA data centre is used by non-EEA cloud provider / customer?
  - How does exemption for mere ‘transit through’ an EEA state apply to:
    - ‘follow the sun’ backup arrangements?
    - incidental processing in the context of cloud load management?

Where do European data protection laws reach to (2)?

- Might there be a regulatory gap if an entity uses equipment / means in the EEA but also has an [irrelevant?] establishment in the EEA?
- What are the implications of the March 2011 decision of the French DP regulator [CNIL] to exempt from certain obligations (inc. re-export of data) processing by French service providers on behalf of non-EEA customers?
- Can a cloud customer control where its data are stored in the clouds?
  - Sometimes no choice
  - Regional choice may be offered - but what is contractual status?
  - Sometimes locally by default
  - Sometimes negotiable

Current issues with EU approach to applicable law

- Even within the EEA, data centres and network architecture may trigger multiple compliance regimes + conflicts due to lack of harmonisation
- Practical consequences include…
  - Inconsistent filing / notification / approval requirements
  - Inconsistent application of the test of ‘establishment’
  - Inconsistent scope *eg* special category data / corporate persons
  - Inconsistent security requirements *eg* Italy v UK

Inside the matrix – a few of the many permutations…

	Cloud customer	Cloud provider	Data centre
1	EEA	EEA	EEA
2	EEA	EEA	Non-EEA
3	EEA	Non-EEA	EEA
4	EEA	Non-EEA	Non-EEA
5	Non-EEA	EEA	EEA
6	Non-EEA	EEA	Non-EEA
7	Non-EEA	Non-EEA	EEA
8	Non-EEA	Non-EEA	Non-EEA
9	EEA	Anywhere	Multiple
10	Non-EEA	Anywhere	Multiple

Queen Mary
University of London
Centre for Commercial Law Studies

Where - the way forward?

- **Short / medium-term options:**
  - EEA (and perhaps other) regional clouds
  - Safe Harbor for transfers from Europe to the US
  - Flexible implementation of EU model clauses
  - Processor BCRs to extend reach of corporate group BCRs
  - BCRs for private / community clouds
  - Encryption as a tool for de-personalising data before transfer
- **Medium / long-term solutions:**
  - Effective DP harmonisation throughout the EEA – even better, the world!
  - End-to-end accountability (*i.e.* promote the Canadian model)
  - Reduce focus on location of equipment where not important
  - Bring DP rules into line with e-commerce regulation?

Queen Mary
University of London
Centre for Commercial Law Studies

"Contracts for clouds: comparison and analysis of the terms and conditions of cloud computing services", Bradshaw, Millard & Walden (2010)

- We reviewed 31 sets of standard T&C (defined broadly)
  - 20 main categories of clause were identified
  - Each set of T&C was then mapped against these categories
  - During the detailed analysis further patterns emerged
- Hypothesis = that where significant variations exist between terms of service, differences would correlate significantly to:
  - Type of service
  - Target market
  - Commercial and technological legacy (if any) of the provider
- Key findings include:
  - Cloud infrastructure and services are often complex (often with multiple dependencies): few contracts reflect this adequately
  - The T&C for particular services can indeed be predicted to a significant extent
  - Many provisions appear to be inappropriate / unenforceable / illegal

Queen Mary
University of London
Centre for Commercial Law Studies

“Off the shelf” cloud computing arrangements

- Many cloud service providers use “click-wrap” terms of business
- Such terms of business may state, for example, that:
  - the service provider has minimal, or even no, liability for loss or damage caused by failure of the cloud computing service
  - subcontracting is unrestricted
  - the service may be modified or discontinued without cause, without notice and without liability to users
  - customers may have limited / no ability to recover data following termination of service
- Depending on the circumstances, the enforceability of some of these terms may be subject to challenge (!)

An example: disclosure of your data to third parties…

Would you feel more comfortable signing up to this…

"The Receiving Party [Salesforce.com] *may disclose Confidential Information of the Disclosing Party* [the customer] *if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure."*

… or this?

"You authorize ADrive to disclose any information about You to law enforcement or other government officials as ADrive, in its sole discretion, believes necessary, prudent or appropriate, in connection with an investigation of fraud, intellectual property infringement, or other activity that is illegal or may expose ADrive to legal liability."

Whose laws apply if you have a cloud dispute?

Choice of law specified by cloud provider…	Number *
US State: California (most common), Massachusetts (Akamai), Washington (Amazon), Utah (Decho), Texas (The Planet)	15
English law, probably because service provider based there	4
English law, for customers in Europe / EMEA	4
Other EU jurisdictions (for European customers): eg. Ireland (Apple), Luxembourg (some Microsoft services)	2
Scottish law (Flexiant)	1
The customer's local law	2
No choice of law expressed or implied, or ambiguous choice (eg. "UK Law" for g.ho.st)	3
** Number in each category is out of 31 contracts analysed by QMUL Cloud Legal Project http://www.cloudlegal.ccls.qmul.ac.uk/*	

Queen Mary University of London
Centre for Commercial Law Studies

Do things actually go wrong?

On 2nd March 2010, G.ho.st sent this email to its users:

Dear Ghost User

> *We hope you have been enjoying our free Ghost service. Regrettably changes in the marketplace mean that it is no longer economical for us to host the Ghost service and we will be closing down the service on or around March 15. We will instead be focusing on licensing or selling our technology to larger companies.*
>
> *We advise you to migrate ALL important folders, files and emails to another secure place before March 15. You might like to consider Google Docs or Microsoft SkyDrive for files and services such as Gmail or Yahoo! Mail for email. Some instructions for migrating data are included below. We are really sorry for any inconvenience this may cause you and are very grateful for the fantastic support we had from our community.*

Contracting in the clouds: custom deals

- Although not generally advertised, major cloud vendors with standard contracts are prepared to go *off piste* if a deal merits it
- One-off contracts are usually confidential but…
- Extensive documentation has been published for the CSC / Google / City of LA transaction, including provisions that depart in significant ways from Google's standard position, *eg*:

  "Google agrees to store and process Customer's email and Google Message Discovery (GMD) data only in the continental United States. As soon as it shall become commercially feasible, Google shall store and process all other Customer Data, from any other Google Apps applications, only in the continental United States." (cl. 1.7)
- We are currently undertaking research on negotiated cloud deals

Practical questions for users of cloud services…

- Is the infrastructure multi-layered and, if so, in what way?
- Where will your data be processed (inc. storage / replication / transit)?
- Who controls the critical infrastructure (and from where)?
- How easily can third parties (public + private) get access to your data?
- What happens if your cloud provider / their provider goes bust?
- How easily could you move your data to another cloud service (or back to your own systems) and how long would it take?
- How confident are you that you could regain control of your data without leaving behind copies and / or key metadata?
- Is the contract OK? (inc. TOS, T&C, SLA, Privacy Policy, AUP, etc)

Queen Mary
University of London
Centre for Commercial Law Studies

Forecast: cloudy and changeable… but bright!

- Putting data / processes into clouds may save money and facilitate risk management but it may also have unintended adverse effects
- Physical location may be highly significant in virtual environments
- Some cloud service providers are more sophisticated than others
- Risks of compelled disclosure and other disruptions are real but are often misrepresented / poorly understood
- It will take time and effort to get regulators comfortable with specific cloud arrangements but increasingly it will happen
- Cloud contracts will evolve rapidly in response to competitive positioning, customer demands and regulatory / judicial intervention

Queen Mary
University of London
Centre for Commercial Law Studies

Thanks for listening!

For background papers please visit:
http://www.cloudlegal.ccls.qmul.ac.uk/

Any questions…

Queen Mary
University of London
Centre for Commercial Law Studies

CILP, University of Toronto

14th October 2011

Cloud Privacy: a European Perspective

Professor Christopher Millard

Centre for Commercial Law Studies, Queen Mary, University of London

www.cloudlegal.ccls.qmul.ac.uk / c.millard@qmul.ac.uk

Queen Mary
University of London
Centre for Commercial Law Studies

Postscript: do “old world” laws apply to online activities?

“Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather… Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter, There is no matter here... We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts...”

John Perry Barlow (Electronic Frontier Foundation)
“Declaration of the Independence of Cyberspace” (Feb 1996)

Queen Mary
University of London
Centre for Commercial Law Studies

Cyberspace and the no regulation fallacy

"There are innumerable law, statutes and regulations which apply to the development, financing, and operation of, as well as the content transmitted via such networks, even though most people who use and operate these networks are unaware of many of the various laws which apply to their activities…"

Millard (1995), "Cyberspace and the 'no regulation' fallacy"
See also Millard and Carolina (1996),
"Commercial transactions on the global information infrastructure: A European perspective"

Queen Mary
University of London
Centre for Commercial Law Studies

Rumours of the death of national sovereignty turned out to be greatly exaggerated…

- Different countries / governments care about different things and to varying degrees but it has long been clear that Barlow's appeal for cyberspace to be left alone was hopelessly naïve. Indeed, when asked in 2004 about that earlier optimism and the "nothing can stop us now" attitude, he simply commented: "We all get older and smarter"
- The Yahoo! Nazi memorabilia case in France (2000-2001) marked a watershed in the assertion of territorial controls over web content
- Targeting based on geo-location technologies is now commonplace as are filtering / censorship / localisation / tax collection…
- See generally: Goldsmith + Wu (2006), "Who Controls the Internet: Illusions of a Borderless World"