Queen Mary University of London, School of Law

Legal Studies Research Paper 191/2015

Policy, Legal and Regulatory Implications of a Europe-Only Cloud

W Kuan Hon

Christopher Millard

Chris Reed

Jatinder Singh

Ian Walden

Jon Crowcroft

Policy, Legal and Regulatory Implications of a Europe-Only Cloud

W Kuan Hon,[*] Christopher Millard,[**] Chris Reed,[***] Jatinder Singh,[****] Ian Walden[†] and Jon Crowcroft[‡][1]

1. Background

1.1 Introduction

There has been on-going discussion regarding the alignment of cloud computing services to a range of European policy objectives. This paper provides an initial outline of some of legal and regulatory aspects arising from recent calls for establishing a Europe-only cloud.[2] Following Edward Snowden's revelations of mass surveillance and data collection by the US National Security Agency ("NSA") and other national intelligence agencies, such concerns came to the forefront with calls for a Europe-only cloud, also referred to as the "Schengen cloud" or "Schengen Internet",[3] apparently involving constraints on the routing of data.[4] Any Europe-only cloud could impact severely on data exchanges between Europe and other regions, such as the US.

In August 2013, German telecommunications provider Deutsche Telekom (DT)[5] and United Internet, who together provide about 2/3 of all German email addresses, announced an "E-mail made in Germany" initiative[6], which would employ only "secure data centers in Germany" for email traffic and

[*] Research Consultant, Microsoft Cloud Computing Research Centre and Cloud Legal Project, both at the Centre for Commercial Law Studies, Queen Mary University of London, UK.

[**] Professor of Privacy and Information Law and Project Leader, Cloud Legal Project, Centre for Commercial Law Studies, Queen Mary University of London and Of Counsel, Bristows LLP. Joint Director of the Microsoft Cloud Computing Research Centre.

[***] Professor of Electronic Commerce Law, Centre for Commercial Law Studies, Queen Mary University of London.

[****] Senior Research Associate, Computer Laboratory, University of Cambridge.

[†] Professor of Information and Communications Law, Centre for Commercial Law Studies, Queen Mary University of London and Of Counsel, Baker & McKenzie.

[‡] Marconi Professor of Communications Systems, Computer Laboratory, University of Cambridge. Joint Director of the Microsoft Cloud Computing Research Centre.

[1] With thanks to Anil Madhavapeddy and Carlos Molina-Jimenez for their assistance and Dan Svantesson and Graham Smith for their comments. This paper was written for, and takes into account feedback from, the Microsoft Cloud Computing Research Centre (MCCRC) Symposium, September 2014: "A Cloud for Europe? Feasibility and Implications of Internet Regionalisation." Both the research presented in this paper, and the symposium at which it was discussed, were made possible as a result of generous support from Microsoft. The views presented herein are, however, the authors' alone.

[2] On key technical aspects, see Jatinder Singh, Jean Bacon, Jon Crowcroft, Anil Madhavapeddy, Thomas Pasquier, W Kuan Hon and Christopher Millard, "*Regional clouds: technical considerations*". Computer Laboratory, University of Cambridge, UK. Tech.Rep.863 (Nov 2014). http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-863.html.

[3] Within the Schengen area, EU citizens may cross state borders freely without being subjected to border checks. This area encompasses all but six of the EU Member States and all four EFTA countries. Of the six EU states that are currently outside Schengen, Croatia and Cyprus are obliged to join and it is a longer-term aim for Bulgaria and Romania also to do so. The UK and Ireland have opted out of the Schengen Agreement and that status is not expected to change in the foreseeable future. It is therefore unclear whether the UK and Ireland would be excluded from any planned Schengen Internet or cloud network.

[4] In this paper we use "routing" in the popular lay sense of routing at the network level, rather than more fine-grained application-specific routing.

[5] Which is 32% owned by the German government - http://www.reuters.com/article/2013/10/25/us-usa-spying-germany-idUSBRE99O09S20131025.

[6] http://www.e-mail-made-in-germany.de/ and see http://www.telekom.com/media/company/192834 (DT's press release announcing this initiative).

use SSL encryption in transmission.[7] This would (according to United Internet's head) make it "impossible for any 'foreign jurisdictions' to gain access".[8] Reportedly they would avoid routing such traffic through US hosted infrastructure.[9] However, this initiative only applies to emails between the relevant German email services,[10] not emails to persons outside Germany,[11] and data at rest on those servers would be unencrypted,[12] leading to suggestions that this move represented "marketing" rather than enhanced protection,[13] and would make Internet use more expensive.[14] That month also, Thierry Breton of European cloud provider Atos (and France's former Minister of Economy, Finance and Industry) proposed "a kind of Schengen" for data.[15] In fact the idea of a kind of digital Schengen area is not new, having been suggested in 2011 by the Presidency of the Council of the EU's Law Enforcement Working Party (LEWP) in the context of cybercrime.[16]

Subsequently, in October 2013, apparently after a private meeting with the German government,[17] DT declared its aim to agree with other Internet providers that German Internet traffic would be routed

[7] http://www.zdnet.com/deutsche-telekom-and-united-internet-launch-made-in-germany-email-in-response-to-prism-7000019266/.

[8] http://www.dw.de/german-companies-to-automatically-encrypt-customers-emails/a-17010661.

[9] http://www.telecoms.com/170312/deutsche-telekom-avoids-us-servers-another-secure-email-shuts/.

[10] N. 7.

[11] http://www.dw.de/germany-looks-to-erect-it-barrier/a-17203480.

[12] Third party access to such data would be granted "only in compliance with German law" (n. 8). Deutsche Telekom started reporting publicly on its provision of information to security authorities in June 2014: http://www.telekom.com/corporate-responsibility/data-protection/More+Articles/239498.

[13] http://arstechnica.com/business/2013/08/crypto-experts-blast-german-e-mail-providers-secure-data-storage-claim/ and n. 19.

There are also reports that the German intelligence agency passes communications metadata information to the NSA in any event, at least relating to non-German citizens. http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.

[14] "…it would be possible to keep email conversations inside German borders. But in doing so, the idea of the fastest and cheapest way would have to be given up. Additionally, investments in network infrastructure would also be required. This could make internet usage more expensive. It would be even more difficult to process the entire internet traffic through domestic lines and intersections. The important Root-Nameservers are mainly based in the US… Setting up a 'national internet [with] an expensive and complex network of servers and infrastructure, like the ones in Saudi Arabia and in Iran, would be needed'" http://www.dw.de/deutsche-telekom-plans-for-a-national-internet/a-17171714.

However, these views are not necessarily accurate, for several reasons. Servers already exist in much European infrastructure (both middleboxes for deep packet inspection (DPI) and caching/proxy, but also large scale content delivery networks (CDNs) - e.g. for IPTV) so there's little cost there. DNS deployment is extremely cheap. Saudi Arabia and Iran run a lot of expensive (US) censorship technology, which seems less applicable in more liberal states in Europe. Work such as P4P aims at traffic localisation (http://www.newsfactor.com/story.xhtml?story_id=032002XVIJS0), meaning that hosting cloud within ISPs would reduce costs. Having traffic leave an Autonomous System that operates a defined routing policy - see further n.2 - incurs peering charges which can be significant, so ISPs are already strongly incentivised to keep traffic local. This also provides lower latency, i.e. better performance and speed, to users. Putting servers further away would be slower – whether it would be cheaper or not would depend. Root servers for .com are mirrored multiple times, but in any case DNS lookups are cached, so once the first lookup has been resolved it's irrelevant where the DNS server is.

[15] http://www.europe1.fr/Economie/Breton-creer-une-sorte-de-Schengen-des-donnees-1620759/.

[16] "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'." http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207181%202011%20INIT para 8. The workability and implications of that proposal were criticised, e.g. http://www.techweekeurope.co.uk/news/eu-proposes-continental-wide-great-firewall-27834.

[17] http://gigaom.com/2013/10/14/why-keeping-internet-traffic-within-borders-is-a-tall-order/ and http://www.technewsworld.com/story/79286.html. Note that the Gigaom article was mainly regarding Brazil, where infrastructure is far less developed than within Europe, and there are vast distances between urban areas compared with in most of Europe. Also, Brazil has deployed far less infrastructure to address this issue than Europe, with very few fibreoptic cables across the Amazon basin, so that many communications are via satellite and thus it can be more efficient (both in terms of time and cost) to route traffic with domestic endpoints (e.g. from

only through domestic connections in order to keep German Internet traffic within German borders),[18] creating a German-only "Internetz",[19] with the next step being to expand this to the Schengen area.[20] It was said that any "national routing" plan would require the commercial cooperation of other such providers including Telefonica and Vodafone,[21] or legislation to compel such cooperation,[22] without which "there is a risk that competitors or users might file lawsuits claiming discrimination or the curtailment of data traffic".[23] Another German Internet service provider QSC queried the proposal's feasibility, stating that it was not possible to determine clearly whether data was being routed nationally or internationally.[24] It has been suggested that DT's proposal was "a public relations move",[25] for political gain or to increase DT revenue.[26] Many ISPs use the *Border Gateway Protocol (BGP)* to manage routing within and between networks under different administrative (ie organisational) control, so it is technically feasible to route in line with the proposed constraints, if ISPs make the appropriate changes both to their technical arrangements and their commercial arrangements regarding their mutual interchange of data.[27] German Interior Minister Hans-Peter Friedrich confirmed briefly in November 2013 that he wanted to "incorporate an IT-Security law in the upcoming coalition agreement that would provide a legal framework for hindering the interception of data exchanged [within Germany and Europe] by foreign intelligence."[28] A draft bill has been published by the German Federal Ministry of the Interior, not mentioning foreign intelligence as such, but including new obligations for technical security measures regarding critical infrastructure, public telecommunications networks and providers of telemedia services, to minimum higher standards, which should help to reduce interception and other security risks.[29]

In February 2014, Germany's Chancellor Merkel met with France's President Hollande to discuss "building up a European communication network to avoid emails and other data passing through the United States… we'll talk about European providers that offer security for our citizens, so that one shouldn't have to send emails and other information across the Atlantic. Rather, one could build up a communication network inside Europe". Hollande's office apparently agreed with the proposals and emphasised the importance of a joint initiative.[30] Merkel was not proposing "a European internet"

Recife to Sao Paulo) via international fibre up to and back from the US. In Europe, "national-only" routing may be complex to configure but would be far more practicable than in Brazil.

[18] "We want to guarantee that no byte between senders and recipients within Germany will even temporarily cross the border". http://www.dw.de/telekom-hopes-to-stave-off-nsa-snoops-by-keeping-internet-traffic-in-germany/a-17154274 The plans were reiterated by DT's then CEO in November 2013: http://www.dw.de/no-welcome-for-deutsche-telekom-national-internet-plans-from-eu-commission/a-17219111.

[19] http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spying-a-933013.html.

[20] N. 3.

[21] http://rt.com/news/deutsche-telekom-internet-spies-176/. Telefonica Germany was said to be "in early discussions on national routing with other groups" while Vodafone was "evaluating if and how" to implement the DT proposal (n. 5).

[22] "Thomas Kremer, the executive in charge of data privacy and legal affairs for the German operator, said the group needed to sign connection agreements with three additional operators to make a national routing possible. 'If this were not the case, one could think of a legislative solution,' he said" (n. 5).

[23] N. 19.

[24] http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html.

[25] N. 5.

[26] http://www.technewsworld.com/story/79286.html.

[27] In practice, routing configuration tends to follow higher-level (typically business) agreements. See n. 2 for more details.

[28] N. 11.

[29] Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). See http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2014/08/it-security-bill.html and http://www.bmi.bund.de/SharedDocs/Downloads/EN/News/informationsheet-it-security-bill.pdf?__blob=publicationFile. This is in advance of the proposed EU Network and Information Security Directive COM(2013) 48 final, with similar aims, which is currently going through the legislative process.

[30] http://www.reuters.com/article/2014/02/15/us-germany-france-idUSBREA1E0IG20140215.

distinct from the worldwide web, but was “looking for an option in which Europeans could use an option in which their data would be stored inside the EU and would not leave Europe”.[31]

German-only routing has been summarised as, “when the sender and recipient of any Internet data are in Germany their data is not sent via another country, as it sometimes is today”,[32] or Europe-only routing envisaged as involving “EU-wide statutory requirements that electronic transmissions between EU residents stay within the territory of the EU… that all data generated within the EU not be unnecessarily routed outside of the EU”.[33]

If these proposals are to progress, what exactly would a “Europe-only cloud” or national cloud entail; how if at all could it be achieved technically and legally, and what would be the consequences?[34] There seem to be two main possibilities regarding the use of any “Europe-only cloud” that is created: require use of only the “Europe-only cloud”, and no other cloud services; or, allow users the choice of whether to use the “Europe-only cloud” or not. It is possible that the two could be combined, e.g. public sector bodies may be required to use Europe-only cloud, but private sector users may be given a choice. Either way, some reliable but flexible method of assuring users that a particular service or provider falls with the “Europe-only cloud” category may also be needed, such as certifications or seals, to supplement any contractual representations.[35]

This paper seeks to lay the foundation for considering the legal and regulatory feasibility and broader implications of a Europe-only cloud. But first, we outline the policy objectives that may underlie the Europe-only cloud proposals.

1.2 Policy issues – why a Europe-only cloud?

A Europe-only cloud approach may seek to meet a range of policy objectives. A chief explicit objective is to prevent unmediated access to European data by foreign law enforcement authorities (LEAs). While the current debate places foreign LEA access as the central policy objective, it should be noted that the Commission’s original cloud communication in 2012[36] refers in Key Action 3 (3.5) to a European Cloud Partnership, stating:

> “The ECP does not aim at creating a physical cloud computing infrastructure. Rather, via procurement requirements that will be promoted by participating Member States and public authorities for use throughout the EU, its aim is to ensure that the commercial offer in Europe is adapted to European needs.”

This illustrates that the "European cloud" debate pre-dates the Snowden revelations.

Another objective might be to encourage domestic cloud providers and develop domestic infrastructure, which others might term economic protectionism or state aid. Protecting European data from foreign LEA access is also couched in terms of protecting fundamental rights from inappropriate interference, particularly rights to private life and to data protection. A related objective could be to encourage the use of cloud computing by European users and the development of a single digital market for cloud computing in Europe,[37] which some might consider they would be more willing to do if they had more confidence and trust that their data would be protected, i.e. based on users’ perceptions of cloud computing and security including LEA access.

[31] http://www.euractiv.com/infosociety/merkel-hollande-lay-foundation-p-news-533560.

[32] N. 46.

[33] Office of the United States Trade Representative, http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf pg. 5.

[34] As the issues are largely similar, in this paper we discuss only “Europe-only cloud”, but much of the analysis will apply to a “German-only cloud” or other national cloud.

[35] See http://ssrn.com/abstract=2441182, 2.4, and http://ssrn.com/abstract=2405971, 4.10.2, and n. 83 pgs. 5, 12.

[36] Commission, Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529.

[37] E.g. the Trusted Cloud for Europe initiative (n. 65).

While some drivers behind policy objectives may be expressly stated, others may remain undeclared. For instance, in relation to the promotion of Europe-only cloud, DT's declared driver is the protection of German citizens' privacy, but it may also be seeking commercial advantage over its US rivals. While a declared driver of many states is the restriction of foreign LEA access, an undeclared driver may be the facilitation of access by the state's *own* domestic LEAs.

Some policy objectives may be in tension or conflict with each other, for example, in relation to fundamental rights, protection of privacy may need to be balanced against freedom of expression, which includes the right to receive information, which a Europe-only cloud may prejudice depending on its scope and implementation. Protection of privacy may also need to be weighed against the policy objectives of economic growth and innovation.[38] Even a single declared objective may in itself encompass a spectrum of possibilities – notably, in relation to access by foreign LEAs, preventing access altogether lies at one end of the spectrum, but controlled access mediated by authorities of the relevant European state seems the more likely objective.

Some policy objectives may be presented as an initial negotiating stance – such as in relation to the current trade negotiations between Europe and the US on a proposed Transatlantic Trade and Investment Partnership (TTIP), to pressurise the US to adopt stronger privacy laws,[39] while refusing to include data protection in the trade talks.[40]

It is therefore important, when considering the meaning, scope, implementation and implications of "Europe-only cloud", to bear in mind the key underlying policy objectives, and to address how they may be achieved and balanced as appropriate. Despite much publicity regarding the risks of access by non-European LEAs and intelligence agencies without going through mutual legal assistance channels, the objective of eliminating such access or making it more difficult is *not* the key focus of this paper, and this paper does not suggest that the technical measures to be discussed can guarantee to prevent such access.

Before the issues can be discussed in detail, however, it is important to clarify what exactly is meant by a "Europe-only cloud". We will therefore now analyse the key constituent concepts in the following order: "cloud", "Europe" and "only".

2. "Cloud"

"Cloud computing" involves many different types of services, and a one-size-fits-all approach should not be taken to the cloud.[41] When "Europe-only cloud" is discussed, what service model is intended to

[38] Ibid.

[39] Former European Commissioner Reding: "I warn against bringing data protection to the trade talks. Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable… Once a single, coherent set of *[data protection]* rules is in place in Europe, we will expect the same from the US… The on-going data protection reform will be the foundation on the European side of a solid data bridge that will link the US and Europe. We expect the US to quickly set its side of the bridge. It is better to have steady footing on a bridge than to worry about the tide in a 'Safe' or, after all, not so 'Safe' harbour." http://europa.eu/rapid/press-release_SPEECH-13-867_en.htm. For more on TTIP see http://ec.europa.eu/trade/policy/in-focus/ttip/about-ttip/.

Contrast negotiations on the multinational Trade in Services Agreement (TISA), where a leaked draft of the Financial Services Annex Art X.11 evinces the aim of facilitating cross-border transfers of financial information: "No Party shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, into and out of its territory, for data processing or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of this Agreement." https://wikileaks.org/tisa-financial/#article_x11.

[40] E.g. http://www.ft.com/cms/s/0/92a14dd2-44b9-11e3-a751-00144feabdc0.html and http://www.euractiv.com/specialreport-eu-us-trade-talks/ttip-data-elephant-room-news-530654.

[41] At its simplest, cloud computing is a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user requirements. W. K. Hon and C. Millard, "Cloud Technologies and Services", in Cloud Computing Law, C. Millard, Ed., OUP, 2013, chapter 1 pg. 3. See chapters 1 and 2 of that book for a more detailed explanation.

be encompassed: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS),[42] or all of them? Furthermore, SaaS services may be vastly different from each other, varying from webmail, photo sharing and social networking to document processing and customer relationship management and more.

Cloud is just one method of delivering and using technology resources, and we suggest that the focus should be on regulating what it is used *for*, not on use of cloud computing per se. There is an important distinction between using cloud computing to make available data *intended to be public*, such as for hosting websites or for providing general online access to public databases, and using cloud computing to store or otherwise process data to which access is intended to be restricted, such as a corporate group's internal customer relationship management data where no one outside the group is intended to have access. Cloud services may also be used for mixed purposes, where some data are intended to be public, but other data are for restricted access only, such as some SaaS storage or social networking services where users may designate certain data or pages public, but intend to make others available only to a defined group of users.

For example, one popular use of IaaS/PaaS is for hosting websites, particularly among organisations that have used cloud for over 18 months.[43] Many websites, including websites of European-incorporated organisations, are hosted using IaaS/PaaS provided by non-European, typically US, cloud providers. A blanket prohibition on using non-European IaaS/PaaS would also ban their use for hosting websites, which seems to cast the net very wide. Surely any requirements regarding "Europe-only cloud" ought to take into account the *purpose* pursued by the underlying policy objective (e.g. to prevent unmediated access by US LEAs), rather than simply targeting cloud computing technology as such. Passing laws requiring local hosting of websites (and web services), which would also be needed in order to ensure Europe-only routing and storage, has been described as "a drastic move that has not yet been pushed by German leaders", but it has been pursued by other nations, such as Indonesia[44] and Russia.[45]

Even if it is possible for Europe to build IaaS / PaaS services that are "Europe-only" throughout the whole supply chain, it must be borne in mind that in reality many *SaaS* services popular with Europeans, whether organisations or consumers, are US-based: e.g. Facebook, Yahoo! Mail, Microsoft Office 365, Google Apps, YouTube and Dropbox, and "if you're using their services, a national routing system will not help".[46] Again, it is not realistic to ban European users from using such services; while any measures would also have severe implications for international trade agreements. If Europeans are to be restricted to using Europe-only SaaS, must Europe produce homegrown

[42] See n. 2.

[43] http://cloudindustryforum.org/downloads/whitepapers/cif-white-paper-8-2012-uk-cloud-adoption-and-2013-trends.pdf#5 and http://www.rackspace.com/blog/top-10-common-uses-for-the-cloud-for-2012/.

[44] Regulation No. 82 of 2012 regarding the Implementation of Electronic Systems and Electronic Transactions.

[45] Federal Law No. 242-FZ dated 21 July 2014 "On Introducing Amendments to Certain Legislative Acts of the Russian Federation with regard to Personal Data Processing in Information and Telecommunications Networks."

[46] http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891. Also: "It would not work when Germans surf on websites hosted on servers abroad, such as social network Facebook or search engine Google" (n. 5). Provisioning such services could include use of servers elsewhere in Europe rather than in the US (which would again involve extra-national routing), as locations of data centres used are not necessarily determined by geographical proximity to customers, "but on factors such as the availability of cheap power, cool climates, and high-speed broadband networks" (ibid).

Certainly, hosting cloud services (whether IaaS, PaaS or SaaS) for European customers in the US would not always be sensible as they incur transit and latency costs. Having data centres near European IXPs (IXPs are discussed in n. 2) means they can be multihomed cheaply to every European national backbone, which would make the BGP configuration easy. But even European-located data centres may be owned/operated by providers that are subject to legal compulsion by non-European states, as will be discussed later. (The reference to "broadband" seems irrelevant as these issues relate purely to access networks available to customers.) See further n. 2.

European equivalents of Facebook, Twitter etc (as well as IaaS/PaaS services)?[47] If so, how can this be achieved?[48]

There are also plenty of other ways for non-European persons to collect and access information about European persons other than through their use of cloud computing; leading to the question of a "Europe-only *Internet*", not just "Europe-only cloud". Many websites, both European and non-European, and whether hosted using cloud computing or not, are known to collect and track personal data of their visitors, often quite detailed. However, the solution cannot be to stop European users from visiting such websites altogether. Even when visiting *European* websites, users may be unable to avoid non-European routing of material automatically downloaded to their computers when visiting the website, because many European webpages may be hosted on servers located outside Europe,[49] and/or may incorporate content and functionality from US providers which will accordingly be routed via the US or other non-European infrastructure, e.g. the Facebook Like button, which enables Facebook to track users' visits to other websites.[50] This is but one aspect of a major limitation, to be discussed further below, to the "Europe-only cloud" concept, which arises whenever *any* non-European service, hardware or related element is included in the service supply chain.

3. "Europe"

What is meant by "Europe", in the context of "Europe-only cloud"? "Europe" could mean the European Union (EU - 28 Member States), European Economic Area (31 Member States), the Schengen Area (26 Member States) or the Council of Europe (47 Member States).[51] In addition, if "Europe" means the EU, the EU has limited competence,[52] such that if a Europe-only cloud was argued for on national security grounds, it would have to defer to Member States to act, who may not trust each other and may differ in their implementations of any measure. Furthermore, if in future any states join or leave the Schengen Area or Europe, any technical means used to achieve a Europe-only cloud[53] would require reconfiguration, which could be very complicated.

At first sight what a "Europe-only cloud" involves might seem obvious, but in fact there are several possibilities here:

- Use only European cloud providers?
- Confine physical location of data to Europe?
- Process data in accordance with European laws?

We will suggest that a key underlying issue is the ***conflation of physical location with access and/or legal jurisdiction***. Arguably this conflation is the key source of many of the problems faced today regarding the application of "legacy" laws to things digital. Legally, there is also a difference between "jurisdiction" and "applicable law". A state may claim that its courts have jurisdiction to hear certain issues, and may claim jurisdiction to apply its laws to certain situations, sometimes even with extraterritorial effect (and in this paper, when we refer to extraterritorial laws or extraterritoriality, we

[47] E.g. "there are too few homegrown alternatives to U.S. services (though admittedly most Germans use German webmail providers)" http://gigaom.com/2013/12/09/outgoing-deutsche-telekom-chief-blasts-eu-and-german-leaders-over-surveillance-inaction/.

[48] "The only way to really make this work would be to gradually promote and strengthen Europe's own technology industry, so that internet users there don't default to U.S. services like they currently do" – Gigaom article (n. 17). Perhaps the Commission's proposals to enable the EU to recognise the potential of big data may help bring this about, e.g. plans to improve EU processing infrastructure. http://europa.eu/rapid/press-release_IP-14-769_en.htm and http://europa.eu/rapid/press-release_MEMO-14-455_en.htm.

[49] N. 5.

[50] Outgoing DT chief executive René Obermann: "many local services such as media websites are in any case plugged into U.S. services such as Facebook and Google, for "social" purposes" (n. 47).

[51] On Schengen, see n. 3. For a Venn diagram showing differences between EU, EEA, and Council of Europe, see http://www.kuan0.com/doc/europe-eea-eu-efta-council-of-europe-venn.html.

[52] Treaty on European Union, Art. 4(2).

[53] Routing, key management and certificate authorities etc – see n. 2.

mean laws that have an extraterritorial *effect*).[54] Courts of a state will not necessarily apply its laws, e.g. when hearing a contractual dispute where the parties have validly chosen to apply the laws of another state to their contract. Many complex issues are raised by conflicts of laws, in situations where multiple states could have jurisdiction or multiple laws could apply – please see further the Appendix to this paper. It should also be noted that national laws may differ widely; even where the laws are a transposition of European instruments; as amply illustrated in the area of data protection.

There is another point to bear in mind throughout this paper. Under EU data protection law, "processing" has a special meaning, and includes passive storage, use, viewing, display, disclosure, transmission etc; "processing" is not limited to active operations on data. However, generally in IT the term is considered to mean active operations on data, i.e. "compute" as opposed to storage or transmission. When we use "processing" or "process" in this paper, it will be in the broadest data protection law sense.

3.1 Only European providers?

Could a Europe-only cloud entail using the services of European cloud providers only, and no other providers? For example, in 2011 the Netherlands government was reportedly going to exclude US cloud providers from government IT contracts handling government or citizen data, “taking into account the possible consequences of the application of foreign law”.[55]

If only “European cloud providers” should be used, which organisations should (or should not) be considered to be “European cloud providers” for this purpose? For example, should it only cover organisations incorporated under the laws of a European state? Requiring use only of providers incorporated in a European state would need to be reconciled with international trade law obligations. A potential analogue for this approach can be found in the Audiovisual Media Services Directive, which defines the concept of ‘European works’ and requires broadcasters to ensure that the "majority proportion" of transmissions is of such works.[56] In addition, while the Directive is a EU measure, the concept of a ‘European Work’ is defined to include the 47 Council of Europe member states, rather than only EU member states. From an international trade perspective, such cultural protectionism is currently permissible, as are measures designed to protect privacy.[57]

What about European-incorporated organisations that are controlled by non-European parents, e.g. European subsidiaries of US technology corporations? Would they be considered to be European cloud providers, or not? Would organisations incorporated outside Europe, but which have physical operations in Europe, e.g. branch offices, be considered “European” for this purpose?[58]

Furthermore, often multiple organisations are involved in the supply chain for a single service, e.g. providers of sub-services and/or of hardware or software used in providing the service. Are organisations considered to be “European cloud providers” only if *all* the sub-providers that they use

[54] "Extraterritorial" jurisdiction in the pure legal sense means where the conduct has no territorial link (e.g. the perpetrator/victim or regulated entity/customers is not in the relevant territory), and therefore a territorial link is established on some other basis (e.g. the nationality of the perpetrator/victim). This should be distinguished from laws that have an extraterritorial "effect", where the conduct *does* have a traditional territorial link, but the regulatee is outside the territory, which is the situation with many of the examples discussed in this paper (e.g. US provider, or Brazilian citizens).

[55] http://www.zdnet.com/blog/btl/dutch-government-to-ban-u-s-providers-over-patriot-act-concerns/58342 And see Kroes: “If European cloud customers cannot trust the United States government, then maybe they won't trust US cloud providers either”. http://europa.eu/rapid/press-release_MEMO-13-654_en.htm.

[56] Directive 2010/13/EU; OJ L 95/1, 15.4.2010, at Arts. 1(n) and 16(1) respectively.

[57] I.e. the WTO’s General Agreement on Trade in Services, at Art. XIV(c)(ii), states that free trade obligations may be subject to exemption for “the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts”.

[58] The Court of Justice of the EU in the *Google Spain* case (ECLI:EU:C:2014:317) ruled that Google Inc., a US corporation, was *directly* subject to EU data protection laws under Art 4. DPD as it had an “establishment” on EU territory by virtue of having a Spanish subsidiary.

to provide their services are “European providers” only too?[59] For example, where a SaaS service is built on a PaaS or IaaS service, must the PaaS/IaaS provider be European-incorporated also (assuming European incorporation as the requirement)? How far down the supply chain is it necessary to look, where would it end, e.g. would a European hardware requirement include the entire manufacturers’ supply chain, down to allowing chips to be sourced only from European chip manufacturers? Must even the operator of the data centre used by the PaaS/IaaS provider (if a separate organisation) be European-incorporated?

Considering lower-level infrastructure, consideration must also be given to the transmission layer, specifically the status of telecommunications providers. Reportedly the German government will not be renewing a contract with Verizon, a US telecommunications provider which provides Internet services to some German government departments.[60] Clearly the concern here is that a state with legal jurisdiction over the non-European provider may compel the provider to disclose data to which the provider has access through its provision of the service.[61] Any routing constraints need to be implemented at the communications infrastructure level, not at the SaaS, PaaS or even IaaS level, so telecommunications providers will have a critical role to play in any Europe-only cloud.

As for suppliers of storage, networking, or indeed computing hardware or software used in the provision of the service, it is well known that both software and hardware may have unintended vulnerabilities which others may take advantage of in order to access data processed using them. They may even have vulnerabilities or “back doors” inserted into them by or at the behest of intelligence agencies.[62] Again, one concern is that a state may be able to do this if it has legal jurisdiction over the provider or even just practical access or control over the hardware, software or standards concerned.[63]

Requiring *all* cloud services, hardware and software to be sourced only from European providers, and no others, may well be difficult to achieve in practice, given that many technology services, equipment and software are operated, supplied or made by non-European organisations, and any such

[59] On difficulties with considering all possible sub-providers and suppliers in the supply chain as “processors” in the data protection law context, see W. K. Hon, C. Millard and I. Walden, “Who is Responsible for Personal Data in Clouds?”, in C. Millard, Ed. (n. 41) chapter 8.

[60] http://www.bbc.co.uk/news/business-28047877 which reported German Interior Ministry spokesman Tobias Plate as saying: "There are indications that Verizon is legally required to provide certain things to the NSA, and that's one of the reasons the cooperation with Verizon won't continue". See also end of n. 111 regarding US organisation Level 3.

[61] Although see e.g. Verizon’s views that the US government cannot compel it to produce customer data stored in data centres outside the US: http://publicpolicy.verizon.com/blog/entry/thoughts-on-foreign-data-storage-and-the-patriot-act.

[62] Cisco’s routers were reportedly intercepted without its knowledge for this purpose - http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/. Some routers are made by Chinese providers like Huawei and it has been noted that lack of spying technology in those cannot be guaranteed either (n. 19).

DT’s “clean pipe” service, through which subscribing organisations may access the Internet, uses LANCOM routers said to involve “‘no backdoor policy’ and incorporates no hidden ways to access its products” and to be “developed and manufactured in Germany and are BSI *[the German Federal Office for Information Security]* certified” – see http://blog.4gon.co.uk/german-network-vendor-lancom-systems-cooperate-on-cyber-security-with-t-systems/ and http://www.techweekeurope.co.uk/news/deutsche-telekom-test-clean-pipe-135510.

[63] Reportedly the NSA deliberately introduced weaknesses into a random number generator used in the 2006 Dual EC DRBG encryption standard http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/?_r=0. The US National Institute of Standards and Technology (NIST) has since removed the algorithm from its draft guidancehttp://www.nist.gov/itl/csd/sp800-90-042114.cfm and a NIST external advisory board released a report in July 2014 stating, “NIST may seek the advice of the NSA on cryptographic matters but it must be in a position to assess it and reject it when warranted... The VCAT recommends that NIST senior management reviews the current requirement for interaction with the NSA and requests changes where it hinders its ability to independently develop the best cryptographic standards to serve not only the United States Government but the broader community.” http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf pg. 7, and see further http://www.nist.gov/director/vcat/cryptographic-standards-guidelines-process.cfm.

requirement could also have public procurement law and trade law implications. Furthermore, this would not guarantee that there can be no access from outside Europe to data handled, as even *European*-produced services, hardware or software may contain unintended vulnerabilities, allowing access by hackers (who may indeed be LEAs) whether from inside or outside Europe; and also, European authorities may choose to communicate European data to foreign authorities.[64] The policy document *Establishing a Trusted Cloud for Europe*,[65] by the European Commission's European Cloud Partnership Steering Board, expressed a clear view on this issue:[66]

> It is clear that the economic potential of European cloud services depends on the ability to avoid any semblance of a "Fortress Europe" model where access to the European cloud market is de facto restricted to providers established in the EU. Non-European cloud providers should be able to access the European cloud market on equal terms, and offer services that adhere to the best practices proposed as a part of the Trust [*sic*] Cloud Europe framework, i.e. functional requirements in relation to data type, data usage and enforceability of European laws and fundamental principles.

This illustrates that the Commission consider the most important issue to be, not the nationality of cloud providers, but whether providers handle data *in accordance with requirements of European laws and principles*, and that such requirements should be enforceable against them.[67] In other words, this suggests their view is that European cloud users should use cloud providers who comply with European laws, whether because they are legally subject to European jurisdiction, or (it seems) because they *voluntarily choose* to comply with European laws in relation to their data processing.

One way may be through adherence to the proposed Code of Conduct for Cloud Service Providers prepared by the Commission in association with various stakeholders in the Cloud Select Industry Group (C-SIG), whose draft is being discussed with European data protection regulators (Article 29 Working Party).[68] An international standard on data protection and security in the cloud in relation to cloud providers has also been issued,[69] although regulators' views on its acceptability under European laws are unknown.

3.2 European physical location?[70]

Another possibility is that "Europe-only cloud" simply means that cloud-processed data must be *physically located* in Europe. This would be consistent with a common approach to "legacy" laws (or their interpretation), which focuses mainly, even exclusively, on the physical location of data. Notably, the DPD restricts the "transfer" of personal data outside the EEA, absent "adequate protection" or exceptions or derogations permitted by the DPD. "Transfer" was undefined but, notwithstanding the

[64] See e.g. http://www.washingtonpost.com/world/europe/germany-looks-at-keeping-its-internet-e-mail-traffic-inside-its-borders/2013/10/31/981104fe-424f-11e3-a751-f032898f2dbc_story.html: "The NSA can reach information even if it is contained exclusively within Germany, said one former U.S. intelligence official", http://rt.com/news/germany-shares-data-nsa-spying-858/ on German intelligence agencies sharing data with the NSA, http://www.zdnet.com/dutch-government-can-use-spy-data-gathered-illegally-court-rules-7000031970/ on Dutch agencies sharing Dutch phone data with the NSA, and http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa on GCHQ, the UK intelligence agency, tapping transatlantic fibre-optic cables landing on British shores carrying data to western Europe from north America, and sharing information with the NSA.

[65] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935.

[66] 60% of respondents to the Trusted Cloud Europe survey agreed with the first sentence, nearly 75% with the second – n. 83 pgs. 7-8.

[67] It is unclear whether this refers to theoretical or practical enforcement. A state could theoretically extend its laws to cover, and claim legal jurisdiction over, persons outside its borders. But if those persons have no tangible connection with that state (e.g. incorporation, people, or assets there), it may have difficulty enforcing against those persons in practice. See further paragraph containing n. 139.

[68] See http://ssrn.com/abstract=2441182.

[69] ISO/IEC 27018:2014 - Information technology - Security techniques - Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

[70] For more detailed explication see http://www.scl.org/site.aspx?i=ed35439.

European Court of Justice's decision in *Lindqvist*,[71] has generally been interpreted by data protection authorities (DPAs) as involving the physical location of personal data "moving" to outside the European Economic Area (EEA),[72] whether by transmission of data to a "third country" outside the EEA, remote access to such data from a third country, or physical transportation to a third country of hardware storing such data. The widespread assumption that physical data location is the most important factor has led to much research being conducted to devise methods to constrain and/or track the physical location of data, e.g. IBM's patent on controlling data location.[73]

Usually, location is taken to mean the geographical location of the *data centres* holding the servers or other equipment in which data are stored or operated upon. However, the "location" of cloud providers is also often mentioned.[74] But what does that "location" mean: the states of incorporation of such providers; the states where they have places of business or operations (which could be different from the state of incorporation, and indeed may be multiple for providers who have operations in several states); or indeed all of them?

If it's necessary to consider the "locations" of cloud *sub*-providers also (whether that be the locations their data centres and/or states of incorporation/operations), then the issue discussed above also arises here - how far down the supply chain must one look? Who must be considered a sub-provider for this purpose: data centre owners/operators, connectivity providers, hardware/software suppliers? And again, what locations must be considered there – their physical places of business/operations, states of incorporation?

Multiple physical locations may be involved in the provision of just one cloud service from a single provider – locations of data centres used not just for persistent storage, but also for active processing operations, for backups or to improve service availability and performance, e.g. caches, content delivery networks / edge locations, or for storage of and operations on *indexes* of stored data and other metadata. Indeed, the physical location of fibre-optic cables used to transmit data between data centres, and between data centre and customer (or cloud provider staff) may also be relevant[75] As we now know, intelligence agencies have intercepted communications through access to physical locations through which cables pass, whether in the USA[76] or outside.

This highlights one reason for the fixation on physical location: there appears to be an implicit assumption that physical location will enable intelligible data to be accessed by whoever has access to that physical location, *and* by states which can compel those persons to access and disclose data to them. However, physical (or even remote) access to storage, computing or communications hardware does not necessarily afford access to intelligible data. This is because the provisioning of cloud services does not necessarily entail that all parts of a particular dataset will physically co-reside in the same hardware or even hardware infrastructure (e.g. data centre). Further, data, whether in persistent storage or in transmission, may be encrypted and/or subject to other protection mechanisms to control who may have access to intelligible data.[77] These mechanisms can work to defeat or hinder access to intelligible data regardless of physical data location. Encrypted data would be intelligible to anyone with access to the data and the relevant decryption keys, but should be

[71] ECLI:EU:C:2003:596. The court in *Lindqvist* decided that uploading personal data to the servers of an EU-incorporated web hosting provider is not a "transfer". It declined to rule on the issue of data location or whether the uploader or provider effected any "transfer" on personal data actually being accessed by a website visitor.

[72] The EEA is the EU plus Iceland, Liechtenstein and Norway. References to "EU" in the DPD context can be taken to include "EEA" as the DPD's application extends to the broader EEA.

[73] http://www-03.ibm.com/press/uk/en/pressrelease/44563.wss - although see prior work such as http://research.microsoft.com/apps/pubs/default.aspx?id=67419. See also n. 2.

[74] Article 29 Working Party, 'Opinion 05/2012 on Cloud Computing (WP196)' 29 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[75] From a DPD perspective, mere transit, i.e. using cables sited in the EU for routing data which do not end up in the EU, does not subject sender or recipient to EU data protection laws for that reason alone: Art 4(1)(c).

[76] E.g. Google and Yahoo's main bridges to the Internet - http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[77] See n. 2.

unintelligible to others. EEA data protection authorities consider that "encrypted data" remain "personal data",[78] whereas we argue that encrypted data should be "personal data" only in relation to those who can access the decryption key (but not those who cannot).[79]

Communications links may also be encrypted, as Google hastened to do for links *between* its internal data centres soon after the relevant NSA revelations.[80] Encrypted links using Transport Layer Security (TLS), e.g. https connections in web browsers, is increasingly recommended – and perhaps becoming the norm, so that unauthorised eavesdropping on transmissions may become less of a problem. However, that assumes a robust encryption regime, and uncompromised and trustworthy key certificate authorities. Thus, again the physical location of providers may be important – in this case, whether providers of the relevant certificates (certificate authorities) are European-based or, for example, US-based.

Furthermore, data physically stored in Europe may be accessed remotely. As such, a focus on “location” could involve multiple locations here too – e.g., the state where the person who accessed data was physically located at the time of the access; even the state of which that person is a citizen or resident or (if the access is attributable to an organisation) in which the organisation was incorporated. Indeed, actual remote access to personal data physically stored in Europe, by someone then physically located outside Europe, is in practice generally treated by many practitioners and DPAs as a regulated “transfer” of that data to a location outside Europe for DPD purposes. Such remote access could be by an authorised person, but it could also be unlawful, e.g. criminal hacking. But whether data physically stored in Europe (or outside) is protected against hacking or other unauthorised access depends on the security measures deployed, not on the physical location of the data. Physical location of data in Europe does not protect it against unauthorised access. In terms of controlling access to data, *security* measures such as access control and encryption, including control of keys[81] are more important than physical location to restrict access to persons or to an extent not authorised by the cloud customer. Physical location is relevant to security, but only as one element, rather than as an end in itself.[82] Thus, 93% of respondents to the Trusted Cloud for Europe survey supported the idea of encouraging “information security that is balanced with consumer and provider needs”, while 68% supported review and identification of formal requirements (e.g. data location) and underlying functional requirements (e.g. security and accessibility) that could serve as acceptable substitutes.[83]

To recap, physical location of data in Europe is not always necessary or sufficient for ensuring that the data will be protected and handled in accordance with European laws.[84] We argue that the continuing narrow focus on physical data location obscures the underlying issue: namely, access to intelligible data, and the importance of security measures in that regard. Furthermore, this focus is not necessarily consistent with a decision of the EU Court of Justice, which emphasised *jurisdiction* over physical location.[85] Indeed, regarding national data location restrictions, the Trusted Cloud Europe policy document stated:[86]

> If common requirements can be found for similar use cases, Member States can choose to gradually phase out data location restrictions when they are deemed unnecessary. This does not imply that data controls should be abandoned; it is often possible and advisable to replace

[78] N. 74.

[79] See W. K. Hon, C. Millard and I. Walden, “What is Regulated as Personal Data in Clouds?” in C. Millard (Ed.), Cloud Computing Law (OUP, 2013), chapter 7.

[80] http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html.

[81] Covered in more detail elsewhere - see n. 2.

[82] W. K. Hon and C. Millard, “How Do Restrictions on International Data Transfers Work in Clouds?”, in C. Millard, Ed., chapter 10, and n. 70.

[83] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6608 pgs. 4-5.

[84] N. 82 and n. 70.

[85] *Lindqvist* (ECLI:EU:C:2003:596) and n. 70.

[86] N. 65, pg. 19.

> formal legal requirements (such as geographic location of the data) by the corresponding functional requirements (such as ensuring the accessibility and security of the data). State-of-the art security technologies could be regarded for some use cases as an alternative to data location restrictions. This goal oriented approach is technologically neutral, conducive to supporting innovation and new technologies, and enables public policy objectives to be more effectively reached.

Brazil decided to drop a requirement proposed in autumn 2013, after the Snowden revelations, to store all information regarding Brazilian citizens locally, only in servers physically located in Brazil, i.e. to ‘oblige internet service companies […] to install and use centres for the storage, management and dissemination of data within the national territory’.[87] The “forced data localisation” proposal was criticised on the basis that requiring providers to build/use data centres/servers in Brazil would increase costs significantly for users, “scare Internet companies away”, not guarantee protection against nefarious actors to whom location of Internet-connected computers is irrelevant and who may intercept data if routed over the Internet, and make surveillance of Brazilian citizens easier for Brazil’s police and intelligence services.[88] When passed in April 2014[89] the law (commonly known as Marco Civil da Internet, and now in effect) instead applied Brazilian law extraterritorially, extending Brazilian *jurisdiction,* including requirements to meet LEA requests, even to *non*-Brazilian organisations in relation to information on Brazilian citizens, wherever stored.[90] Extending the territorial reach of national laws has been a strong trend over recent years.[91] The UK recently passed The Data Retention and Investigatory Powers Act 2014 (DRIPA),[92] under which non-UK service providers holding communications data of UK citizens, particularly webmail providers, could be forced to retain and disclose their data (s 4).

Russia’s new law,[93] amending its personal data protection law,[94] requires that “while collecting personal data, including by means of the internet, an operator should provide recording, systematization, storage and update of the Russian citizen’s personal data using databases located in the territory of the Russian Federation”,[95] with certain exceptions e.g. “personal data processing for the purpose of implementation of an international agreement or related Russian law”.[96] The locations of servers hosting such databases must be notified to Roskomnadzor (the Federal Supervision

[87] http://dataguidance.com/news.asp?id=2129.

[88] See e.g. http://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html - and see also n. 17.

[89] http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm.

[90] More specifically, any data processing operation involving logs, personal data or communication where at least one processing activity (for example, collection or storage) occurs in Brazilian territory will be subject to Brazilian rules on privacy, data protection and secrecy of private communications and logs. This will be the case when at least one of the devices connected to the Internet is located in Brazilian territory (even if the organisation carrying out the data processing activities is located outside), provided the activity offers a service to the Brazilian market or at least one member within its economic group has an establishment in Brazil. Monica Salgado, ‘New Data Protection Law in Brazil’ [2014] Privacy & Data Protection 13.

[91] See I. Walden, "Law Enforcement Access to Data in Clouds" in Cloud Computing Law, C. Millard, Ed., OUP, 2013, chapter 11 pg. 285.

[92] http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted/data.htm.

[93] No. 553424-6 http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=553424-6.

[94] Initially this law, signed by Russia's President Putin on 21 July 2014 (previous note), was to take effect on 1 September 2016. However, reportedly an amendment bill submitted to the State Duma, the lower house of Russia's Parliament, on 1 September 2014, cited 1 January 2015 as the effective date e.g. http://www.bna.com/russia-seeks-new-n17179894570/. It has also been reported that the State Duma approved the draft amendments on 24 September 2014 in a second reading, but a third reading, signing by the President and official publication is necessary before they can take effect. http://www.globallawwatch.com/2014/09/russias-new-law-establishing-localization-requirement-for-processing-of-personal-data/.

[95] http://en.itar-tass.com/russia/739029.

[96] http://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/7/Russias-Internet-Privacy-Act-will-have-wide-implications-for-foreign-companies/.

Agency for Information Technologies and Communications).[97] Furthermore, non-compliant services may be added to a "blacklist" register of domain names, network addresses and webpage indexes[98] maintained by Roskomnadzor, and Russian authorities are empowered to require restriction of public Internet access to such services.[99] Effectively, the law will prohibit non-Russian cloud and other Internet service providers (including search engines, social networks, mobile app providers and web hosts) from providing online services that involve processing personal data of Russian citizens, including email addresses and emails, unless they create databases of such data on Russian-located servers,[100] which would entail establishing data centres in Russia or using Russian data centres, with associated costs implications and tight timing even for Russian providers.[101] Practical compliance may also be unclear regarding Russian citizens living outside Russia,[102] and how providers can verify the nationality of data subjects and whether the law will apply to them if data on nationality is not available.[103] More generally, Russia's Association of Electronic Communication (RAEC), a lobbying group for Internet organisations, warned that "many global internet services would be impossible"[104] and Russian search engine Yandex reportedly considers the law "…another step towards the strengthening of state control over the Internet in Russia, which has a negative impact on the development *[sic]* industry".[105]

Whether this law would achieve its goals depends on the true nature of those goals, which seem unclear.[106] It has been suggested this move seems designed more to facilitate Russia's *own* access to its citizens' data for the benefit of its intelligence and law enforcement agencies,[107] whereas currently Russia would need to submit mutual legal assistance requests to obtain data from other states.[108] Even so, encryption of such data may prevent, hinder or delay such access, although Russian government authorities may well have the resources to decrypt specifically-targeted data. An avowed objective of Russia's new law is to prevent or at least impede digital access to such data by persons outside Russia, particularly non-Russian intelligence agencies.[109] However, this could be defeated relatively easily because remote access to such data from outside Russia is technically possible over the Internet, and providers (Russian or non-Russian) subject to another jurisdiction's laws may be compelled to retrieve such data e.g. by warrant.[110] Even data stored in Russia, if

[97] N. 93 and http://www.techweekeurope.co.uk/news/russian-government-will-force-companies-store-citizen-data-locally-148560.

[98] It is unclear how webpage indexes would be registered.

[99] Nn. 95, 96.

[100] Nn. 95, 96.

[101] Popular Russian search engine Yandex is reportedly already using Russian servers, but added that "building data centres required by law from scratch would take more than the two years allocated" http://www.techrez.com/2014/07/russia-internet-restrictions.html. Other Internet organisations also consider 2 years is insufficient to find or build Russian data centres (n. 94).

[102] E.g. http://tech.slashdot.org/comments.pl?sid=5365111&cid=47387219.

[103] http://www.alrud.com/upload/iblock/3ea/Newsletter_Ban%20to%20store%20personal%20data%20outside%20Russia.pdf.

[104] E.g. http://news.yahoo.com/russian-lawmakers-pass-bill-restricting-internet-172456389.html.

[105] http://www.cnet.com/uk/news/facebook-gmail-skype-face-russia-ban-under-anti-terror-plan/.

[106] E.g. http://techcrunch.com/2014/07/02/russia-moves-to-ban-online-services-that-dont-store-personal-data-in-russia/.

[107] E.g. http://nakedsecurity.sophos.com/2014/07/04/russias-latest-internet-law-proposal-anti-nsa-or-pro-fsb/, and n. 105. And on German-only email routing, see n. 14: "So you would [in effect] have a national surveillance of the internet… That also applies if only the email communication, not the total internet traffic, stays in Germany. It might avoid foreign intelligence services reading it but it would allow the German intelligence services easy access".

[108] See n. 91.

[109] MP Vadim Dengin reportedly stated, while introducing the bill to Russia parliament, that organisations should build data centres in Russia: "Most Russians don't want their data to leave Russia for the United States, where it can be hacked and given to criminals. Our entire lives are stored over there" (n. 101). Another possible motivation could be to encourage development of Russian online services.

uploaded, downloaded, or otherwise transmitted over the Internet, may be intercepted by persons from other states. Which brings us back to the wider Internet physical routing issue.

A fair question to ask is, to what extent *are* European Internet communications actually routed through the USA or otherwise outside Europe, currently? A 2001 report for the European Parliament noted, regarding cable communications, that:

> At the time of the science backbone, the switches for the routing of global Internet communications were situated in the USA. For that reason, at that time intelligence services could intercept a substantial proportion of European Internet communications. Today, only a small proportion of intra-European Internet communications are routed via the USA. A small proportion of intra-European communications are routed via a switch in London to which, since foreign communications are involved, the British monitoring station GCHQ has access. The majority of communications do not leave the continent: for example, more than 95% of intra-German Internet communications are routed via a switch in Frankfurt."[111]

Mechanisms to restrict physical location of data and/or routing may be feasible technically.[112] Indeed, some providers already process, or offer the choice of processing, customer data in data centres located geographically close to users, to reduce latency – often for performance and availability rather than legal reasons.[113] However, for national or Schengen routing of data, as well as addressing various technical issues,[114] the involvement of multiple Internet providers would be needed, whether

[110] A New York magistrate judge's warrant against Microsoft for email data stored in Ireland has been much publicised and Microsoft's appeal was supported by Apple, Cisco and Verizon. See e.g. http://www.v3.co.uk/v3-uk/news/2350252/apple-and-cisco-lend-support-to-microsoft-in-cloud-data-access-debate Microsoft lost the appeal, and is being given time to appeal further, which it is doing. http://techcrunch.com/2014/07/31/microsoft-loses-email-privacy-case-with-u-s-gov-will-appeal/ and http://blogs.microsoft.com/on-the-issues/2014/07/31/microsoft-responds-ruling-warrant-case/.

However, it is not only the USA where government authorities ask foreign providers for data stored abroad, e.g. Brazilian court orders against Google in 2006 for data (including IP addresses, names and email addresses) stored on US servers relating to users of Google's social network Orkut. http://www.informationweek.com/google-wrestles-with-brazils-requests-for-user-data-on-american-servers/d/d-id/1046450 and http://www.washingtonpost.com/wp-dyn/content/article/2006/09/01/AR2006090100608.html.

[111] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN [3.3.1.1]. According to a board member of the non-profit organization that runs the DE-CIX Internet exchange point in Frankfurt, in a report regarding DT's proposal, "More than 90 percent of Germany's internet traffic already stays within its borders" (n. 5). This percentage was confirmed by DT's head of security - http://www.dw.de/no-welcome-for-deutsche-telekom-national-internet-plans-from-eu-commission/a-17219111 - but another source stated that "only around 40 percent of German Internet traffic is conducted between domestic computers *[apparently meaning, servers owned by German organisations?]*… But some Internet service providers also use American providers, such as Level 3 Communications, for data transfer. That means that even if the actual bits never leave Germany's borders, the NSA could (potentially) still access them, although the company vehemently denies this." (n. 19). The ultimate source of these figures is unclear, and they may be difficult to verify, especially as much traffic is HTTPS and cached nationally.

[112] E.g. NIST's proof of concept on "trusted geolocation for deploying and migrating cloud workloads between cloud servers within a cloud" http://csrc.nist.gov/publications/drafts/ir7904/draft_nistir_7904.pdf.

[113] E.g. Heroku http://gigaom.com/2013/04/25/heroku-comes-to-europe-but-data-protection-issues-remain/. Other providers do allow customers to choose European data centre locations for regulatory reasons, e.g. Microsoft and recently Amazon https://aws.amazon.com/about-aws/whats-new/2014/10/23/announcing-the-aws-eu-frankfurt-region/.

[114] E.g. "It would need its own root DNS servers and its own designs for address allocation as well as a protocol to hand off traffic to the Internet at large… government funding and the network would require maintenance and - possibly – monitoring in the form of deep packet inspection just to ensure network efficiency". http://www.technewsworld.com/story/79286.html.

However, see n. 14. It is not difficult to run DNS servers. All ISPs already conduct deep packet inspection as they need to do so for traffic engineering their own internal server/client traffic. Most European ISPs have local-only CDNs (e.g. Telefonica and BT have such CDNs for IPTV services). Further, DNS inherently supports delegation, enabling a decentralised namespace, and IP address allocations are also delegated, so "own designs to address allocation" and "protocol to hand off traffic" would seem not be difficult, or even necessary.

through voluntary cooperation or legal compulsion.[115] Geographical routing may also be specifically designed to circumvent legal controls. For example, US authorities apparently deliberately routed traffic between US citizens outside the USA in order to get round US laws that forbid interception otherwise.[116] The UK considers that its security services are entitled to monitor searches on US cloud services Google, Facebook, Twitter and YouTube, as well as supposedly private messages on social media among UK citizens, and emails to or from non-British citizens abroad, on the basis that they are deemed to involve "external" communications.[117]

There are also limitations with trying to constrain physical location or routing, as mentioned above regarding emails sent to recipients in another state, or where services or hardware/software used are controlled by providers (including certificate authorities) who are subject to foreign jurisdictions,[118] who may be legally compelled to access and disclose data: "The point of a German-only Internet becomes moot… the moment a customer uses services, such as Google, that transfer their data traffic using foreign infrastructure and thereby renders it subject to the laws of those states."[119] Indeed, a DT representative acknowledged that "If users access services outside of this national - or Schengen - routing system (we propose expanding the system to the Schengen Area), then it won't work. The data will have to be exchanged with that in the United States, and then American regulations apply", and also, "in order to access your data while abroad, you will have to go over foreign networks".[120]

Furthermore, the argument that confining physical location and routing of data to Europe would prevent foreign LEAs from gaining access to European data lacks substance,[121] because they may such gain access from *European* authorities, who can access such data (as national laws allow for national security and/or law enforcement purposes, to varying extents), and may choose to pass such data on to foreign authorities.[122] No one has ever suggested that foreign LEAs should never obtain access to European data, simply that to do so they should go through mutual legal assistance procedures under relevant treaties e.g. the Council of Europe Convention on Cybercrime (2001).

National or Schengen routing proposals have encountered considerable scepticism, with Pirate Party MEP Amelia Andersdotter terming Friedrich's proposal "trumped-up lip service… and it's ineffective, and it's hypocritical", pointing out that it is the overall Internet "infrastructure that creates insecurity… The spying we've seen is an egregious violation of human rights. Why should we believe that the limitation of internet traffic to Germany and Europe means the problem is solved?". An expert from Europe's largest hacker association, German-based Chaos Computer Club, has noted that while the "infrastructure needed to create an inner European network exists", "[b]y 'ensuring' citizens that they are only safe if they restrict their internet usage to within Europe, what is the Internet there for?"[123]

[115] N. 19. "Deutsche Telekom could also have trouble getting rival broadband groups on board because they are wary of sharing network information", and "Others pointed out that Deutsche Telekom's preference for being paid by other Internet networks for carrying traffic to the end user, instead of "peering" agreements at no cost, clashed with the goal to keep traffic within Germany. It can be cheaper or free for German traffic to go through London or Amsterdam, where it can be intercepted by foreign spies" (n. 5).

Whether this is the case depends on specific arrangements. Generally, the aim is traffic localisation to reduce latency and transit costs, e.g. there is often a tight coupling between major infrastructure and service providers (see n. 2).

[116] http://ssrn.com/abstract=2460462.

[117] http://www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr and http://www.theguardian.com/world/2014/jun/18/government-surveillance-watchdog-loopholes.

[118] Such as foreign social networking services, even European websites that incorporate scripts or plugins or other functionality from foreign services - see §2.

[119] N. 19.

[120] N. 46.

[121] As stated by a DT spokesman regarding national routing: "Secret services of states outside this area would then find it much more difficult to access this data traffic" (Gigaom article n. 17). Note that he did not say "impossible" – see also Washington Post article n 64 : "Routing German Internet traffic within Germany "makes it a little more difficult for the NSA to look into our data... But… The solution is not really technical. The solution is a political one".

[122] N. 64.

[123] N. 11.

Similarly, “The initiative runs counter to how the Internet works today - global traffic is passed from network to network under free or paid-for agreements with no thought for national borders…. It is internationally without precedent that the internet traffic of a developed country bypasses the servers of another country”.[124] Even DT’s outgoing chief executive has acknowledged that “proposing a ‘German internet’ would be like asking for a “German sun.”[125]

Others have expressed concerns about economic as well as openness implications: “If more states wall themselves off, it could lead to a troubling ‘Balkanisation’ of the Internet, crippling the openness and efficiency that have made the web a source of economic growth”,[126] and “you can create regulations that block off trade in these information services… *[but]* There will be massive sacrifices of economic efficiency”.[127] Human rights law is also relevant. It looms largest in this context in relation to privacy and data protection under the DPD and the EU Charter of Fundamental Rights,[128] but rights to freedom of expression and information, and indeed even to liberty and security, freedom of thought, of the arts and sciences, to education and to work, could be affected depending on how a Europe-only cloud might constrain access by European citizens to non-European data or services.

Significantly, former Commissioner Kroes (responsible for the Digital Agenda) reportedly was not positive about the concept of a German Internet, stating in similar vein that “Telcos are too important to have only a ringfenced fragmented approach.[129] We can't afford to have 28 member states just ringfenced… We have to compete with global partners and we have to take into account that our cost level can be reduced and that that [*sic*] at the end of the day is beneficial for the citizens”,[130] She also stated, “The global market cannot be conquered when data is caged within national boundaries and their legal framework”,[131] and “if cloud services are denied scale, they become more expensive. For example, if individual states work disjointedly on separate national clouds, then the potential is lost.”[132] However, she also seemed to cautiously welcome some aspects of the Europe-only cloud initiative: “We support Chancellor Merkel’s calls for better networks, and better data protection and security on those networks, as part of a broader digital industrial policy... “We hope that that Franco-German discussion on Wednesday, and the discussion with leading industrialists, will lead to an acceleration of work on important European legislation in this domain”.[133]

3.3 Process under European laws?

A third possible interpretation of a “Europe-only cloud” is that any processing of “European data” using cloud computing should take place in compliance with European laws and principles,[134] *regardless* of the physical locations of data,[135] or the providers’ or sub-providers’ places of

[124] N. 5.

[125] N. 47.

[126] N. 5 and http://www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web.

[127] http://www.npr.org/blogs/parallels/2013/10/16/232181204/are-we-moving-to-a-world-with-more-online-surveillance.

[128] http://ec.europa.eu/justice/fundamental-rights/charter/.

[129] Ironically, this is exactly what EU telecoms law currently does, because Member States have not accepted the “country of origin” principle, whereby a provider is to be regulated by a single Member State, that from which it originates.

[130] http://www.dw.de/no-welcome-for-deutsche-telekom-national-internet-plans-from-eu-commission/a-17219111.

[131] N. 14.

[132] N. 55 (Kroes).

[133] http://gigaom.com/2014/02/17/after-us-squashes-no-spy-hopes-european-leaders-discuss-ways-to-protect-citizens-data/.

[134] Germany’s Chancellor Merkel has said US internet companies must abide by German laws and tell officials what they are doing with citizens' data. "Germany will make clear that we want internet firms to tell us in Europe who they are giving data to”. http://www.wired.co.uk/news/archive/2013-07/15/angela-merkel-prism.

[135] Illustrating difficulties with understanding what laws require in relation to physical data location, in a case striking down the EU Data Retention Directive as contrary to fundamental rights due to its wide scope and lack of provision for appropriate safeguards, the Court of Justice of the EU stated (para 68):

> “it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3)

incorporation or operations. This seems to us to be the most technologically-neutral way to address the fundamental underlying concern, and here we use "European data" simply to mean data that Europe decides should be subject to European laws; although this is another concept that requires detailed analysis and consideration by policymakers, particularly which data (e.g. European citizens) and in what circumstances.[136]

A major concern that states have regarding data is that processing of "their data" (which we use analogously to "European data") should be subject to their own laws and jurisdiction. Some states apply their laws based on physical location in their territory of data, or at least of equipment used to process data; for example one jurisdictional ground under Art 4 of the DPD is based on equipment location. One priority motivating Brazil's desire to require local storage of data was "so that it could be subject to Brazilian laws",[137] illustrating the conflation of physical location with jurisdiction to enforce a country's laws effectively. Unsurprisingly, that approach is rooted in the pre-digital world, where states can have effective jurisdiction over persons or physical objects located on their territories. That approach may make sense with things physical, but not with *digital* data, which are relatively easy to duplicate and copy/move between physical locations, and where multiple copies of the same data may exist in different locations. Indeed, recognition of this reality drove changes to the DPD's jurisdictional basis, from data location in the original 1990 draft, to equipment location in the 1992 amended proposal.[138] No doubt the relative ease of exercising jurisdiction over equipment physically located in one's territory and the relative stability of equipment's physical location, compared with more "movable" digital data, was a factor. Brazil achieved its own jurisdictional aim, even after dropping the local data storage requirement, by extending its laws to apply with *extraterritorial effect* instead. So, in terms of jurisdiction, states can attempt to apply their laws territorially or extraterritorially, but even territorial jurisdiction may have extraterritorial *effects*. Art 4 DPD provides for global application of EU national data protection laws, theoretically, in two distinct ways. Firstly, it regulates processing of personal data worldwide by an entity established in an EEA Member State to the extent that such processing is "in the context of the activities" of that EEA establishment. Secondly, it applies national laws to entities who use "equipment" in EEA territory to process personal data, such as operators of non-EEA websites who set, read or modify cookies on visitors' computers or mobiles located in the EEA (being "equipment"). As for practical enforceability, *Google Spain*[139] is again relevant. Here, the EU Court of Justice found that US-based Google Inc's activities in relation to Google Search were regulated under Spanish law because those activities were "inextricably linked" to the sales activities of Google's Spanish subsidiary.[140]

If a state has effective[141] jurisdiction over a person who controls such access (regardless of the data's physical location), then it has the ability, in practice if not always in accordance with its international law or treaty obligations, to regulate how such data are processed, including use and/or disclosure. This practical ability implicitly underlies and enables requests by a state's authorities, made to

> of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data".

This unclear passage has seen different interpretations, e.g. that such data cannot be retained outside the EU because (in the court's view) it could not be controlled by an independent authority in that situation, or that (our preferred interpretation) such data *can* be retained outside the EU provided that it is subject to such independent supervision, which could be by a non-EU authority such as the US Federal Trade Commission.

[136] The draft Data Protection Regulation refers to personal data of "residents" of Member States or data subjects "residing" in the EU, which concept is undefined and may be problematic – see e.g. Dan Jerker B Svantesson, 'A "Layered Approach" to the Extraterritoriality of Data Privacy Laws' (2013) 3 International Data Privacy Law 278, 279.

[137] http://www.reuters.com/article/2014/03/19/us-brazil-internet-idUSBREA2I03O20140319.

[138] N. 70, text to fn 7-8.

[139] N. 58.

[140] N. 58, paras. 55-56.

[141] Whether jurisdiction claimed by a state is *effectively* enforceable in practice is a different issue, particularly when it attempts to apply its laws extraterritorially (n. 70, text to fn 35). Extraterritoriality is discussed further below.

persons incorporated or doing business in that state (or otherwise under its jurisdiction), for data physically located elsewhere but to which the person has intelligible access.[142] It certainly underlies ongoing concerns that US authorities may obtain European personal data through US cloud providers or sub-providers, but again those assume that such providers will necessarily have access to intelligible data, which may not always be the case, e.g. such access could be excluded by customers encrypting data securely before upload to the cloud (and managing the keys securely, including ensuring providers do not have access to the keys).[143]

All this suggests a different possible approach. The Commission's communication on cloud computing in 2012 seems to have envisaged this interpretation of "Europe", with "European needs" meaning "in accordance with EEA laws".[144] Accordingly, it may be possible to seek to apply European laws to certain data that are not intended to be public, but where access is intended to be available e.g. only to employees of a particular organisation or group, not by constraining the data's physical location to European territory, but by requiring that only those who are subject to European jurisdiction may have *access* to that data, especially in intelligible form. Although commercial motivations may have hindered their adoption in practice,[145] such access restrictions to enforce a kind of "virtual jurisdiction" may be implemented through technical measures. This approach seems the most promising, in our view, as regards cloud data intended for restricted access. For data intended to be public, e.g. published on a website, which is one of the possible uses of cloud computing, obviously such an approach is not relevant or feasible: the discussion here centres only on technical measures to enforce "virtual jurisdiction" regardless of physical location, in relation to cloud data intended for limited access, which is the case for many organisations' uses of cloud computing.

As such, the use of Information Flow Control (IFC) techniques may enable data and context-specific requirements to control data access and continuously control data flows according to application-level policy. In outline, data could potentially be tagged to indicate not only ownership but also type (e.g. medical, company, personal), state (encrypted, anonymised, user-input), location and jurisdiction, upon which information management policy (at a technical-level) can be based. IFC for cloud computing is on-going research: we are designing, developing and implementing a prototype to explore this.[146] In addition, encryption is also highly relevant as it renders information unintelligible for all those without the requisite keys. This, again, emphasises the importance of information security. Implementing appropriate security measures can, depending on the particular technology, help to protect against access to intelligible data by unauthorised persons, whether hacking by cybercriminals or lawful (or unlawful) direct access by foreign authorities.

The latter risk may be mitigated by implementing technical security measures to restrict access to intelligible data to authorised persons, which may include access controls, limiting the rights of authorised persons to the minimum they need for their jobs, and encrypting data to prevent such access even by service providers, such as SaaS storage providers, etc. Ideally, access even to encrypted data, and distribution of copies of encrypted data, should also be restricted as far as possible.[147]

[142] Such as the US warrants and Brazilian court orders against Microsoft and Google respectively – n. 110.

[143] See n. 2.

[144] N. 36 and accompanying text.

[145] E.g., Google generates revenue by displaying advertisements to Gmail users that are targeted based on the content of their emails; if emails were encrypted so that Google's software could not "understand" their content, Google's ability to monetise user content in this way would be reduced. However, Google and other cloud providers are increasingly encrypting data and communications links following the Snowden revelations, prompted by the perhaps greater spectre of lost business from non-US customers distrustful of whether their data are safe from US intelligence agencies' "snooping". E.g. http://rt.com/usa/163600-google-encryption-tool-nsa/. If such providers are applying the encryption they will still be able to access the data themselves, in keeping with their business models, and also may disclose data in response to court orders, but at least such encryption should hinder authorities' direct interception of intelligible data without providers' knowledge.

[146] In conjunction with CloudSafetyNet: End-to-end application security in the cloud" EPSRC Jan 2013 - Dec 2015 http://www.cl.cam.ac.uk/research/srg/opera/projects/csn. See n. 2.

[147] See n. 2.

The former, the risk of states exercising jurisdiction over persons authorised to access intelligible data, may enable states to regulate the processing of that data wherever located, and seems more practical than basing jurisdiction on physical location of data, but potentially allows states to extend their jurisdictional reach to data physically located outside their territories. The extent to which states *should* claim jurisdiction over such processing or data when the interests of other states are involved, and how, will be discussed next.

4. "Only"

We now come to the "only" of "Europe-only cloud", which we believe is, from a legal viewpoint, the crux of the fundamental problem underlying many unsatisfactory attempts to apply pre-digital laws to the cloud, and indeed the Internet more generally: that of multiple applicable jurisdictions and conflicting laws. The problem here is that many organisations may be subject to European laws – but, in today's globalised world, they may not be subject *only* to European laws, particularly when digital data are involved. European organisations, particularly those that operate multinationally, will be subject to the laws of several states simultaneously. Similarly, if a non-European multinational organisation uses "Europe-only cloud" services, it would also be subject to multiple jurisdictions. Accordingly, it is not generally possible to guarantee European-only jurisdiction unless that jurisdiction is *exclusive*, which is not usually the case.

When different states claim jurisdiction over the same organisation and, more specifically, its data processing, and complying with one state's demands would break the laws of another state, the organisation is in the invidious position of having to decide which state's laws to break. Thus, Belgian financial messaging transactions processor SWIFT, which had a second data centre in the USA "mirroring" its European processing, complied with US subpoenas for data processed in that data centre, which EU regulators considered put it in breach of EU data protection laws.[148]

But how do organisations choose which state's laws to break? A major factor may be the nature and severity of sanctions involved, from fines to imprisonment. This can result in a "sanctions arms race" of sorts, as states continue to change the balance of sanctions. As an example, the potentially huge fines (up to 5% of global turnover) under the proposed General Data Protection Regulation that is currently undergoing the EU legislative process.[149]

Jurisdictional conflicts put organisations that operate multinationally in a difficult if not impossible position, including cloud providers and cloud users. This is a broader problem, for which the only long-term solution is international agreement both on the extent to which and manner in which states should be able to claim jurisdiction with extraterritorial effect, and limits, transparency and accountability regarding mass surveillance of their own and other citizens' data. Although the need for such agreement seems widely-acknowledged,[150] the jurisdictional situation is complicated by states

[148] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf. It has since moved its second operating centre to a Swiss location: http://www.swift.com/about_swift/legal/swift_board_approves_messaging_re_architecture.

[149] Discussed in http://ssrn.com/abstract=2405971.

[150] E.g. http://europa.eu/rapid/press-release_SPEECH-14-333_en.htm http://www.npr.org/blogs/parallels/2013/10/16/232181204/are-we-moving-to-a-world-with-more-online-surveillance and http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

increasingly attempting to extend their jurisdictions with extraterritorial effect,[151] and even specifically prohibiting organisations from complying with other states' laws.[152]

How states eventually find a way to reconcile jurisdictional conflicts is beyond the scope of this paper. However, we venture to suggest that it is worth considering whether it would be more sensible to base jurisdiction and conflict issues, not on something as fluid and dynamic as the data's physical location, but on the relevant persons – the persons who control access to intelligible data, and the persons whose data it is (e.g. the data subjects, in the case of personal data). In the Microsoft warrant case,[153] the arguments have focused on the demanded data being stored in a data centre in Ireland, and whether therefore it is beyond US jurisdiction. Yet isn't it equally or even more pertinent to ask whether the account holder, whose data are being demanded, is a US citizen or a citizen of a European state?[154]

5. Concluding remarks

As the above analysis has shown, the basic concern of states and their citizens regarding "their" data is twofold: that their laws, particularly the protection of fundamental rights, apply to such data, and that other states' laws do *not* apply, particularly so as to enable governmental authorities to access that data.

As regards the key legal and regulatory issues raised by the Europe-only cloud proposals, jurisdictional conflicts and extraterritoriality will be highly significant, as will human rights laws and the impact on fundamental rights such as privacy, data protection and freedom of expression. Issues may also arise under competition law and public procurement law. Trade law has already been mentioned, and it should be noted that the implications are multi-faceted. There are implications for *intra*-European trade, competition law and the free movement of services within Europe, particularly if a Schengen cloud or Internet is intended to exclude the UK and Ireland.[155] Furthermore, members of the World Trade Organisation (WTO) will have obligations under the multilateral General Agreement on Trade in Services (GATS), and other WTO commitments. European states have both multilateral and bilateral trade commitments; although some such obligations have provisions designed to safeguard fundamental rights. As such, to the extent that proponents of a Europe-only cloud argue that it is necessary to protect the privacy of European citizens, this may be permitted within the context of existing trade rules.

Finally, the cloud market includes many regulated entities, who may be regulated under different, sometimes overlapping, sector-specific laws, such as information society services and electronic communications service providers. This means that the implications of Europe-only cloud for such entities will differ, depending on the regimes applicable to the relevant entities. Telecommunications law more generally will be relevant, for example whether net neutrality would be undermined by Europe-only cloud.

[151] E.g. Brazil's solution to not requiring data localisation was wide extraterritoriality. Concerns have been noted e.g.: "…the law explicitly applies to any company anywhere that has at least one Brazilian user, has servers located in Brazil, or operates an office there, or effectively, all Internet companies on Earth." http://www.forbes.com/sites/elisugarman/2014/05/19/how-brazil-and-the-eu-are-breaking-the-internet/. Also "If other countries follow this approach… companies like his would have to contend with a bewildering array of national legislation. In some smaller markets, *[Internet firms]* might stop offering services altogether". http://www.economist.com/news/americas/21599781-brazils-magna-carta-web-net-closes. However, in other respects greater extraterritoriality may be positive for international co-operation, e.g. if a UK person hacks into a US server illegally, it might be considered helpful if the US had domestic powers to pursue that person.

[152] As with the "anti-FISA" provision introduced by the European Parliament in the draft Data Protection Regulation – n. 149. The Commission's original proposal also included specific provisions limiting disclosure made in compliance with laws, to those of the Member States and EU law (Art. 6(1)(c) and (3), and Art. 44(1)(d) and (4)). So, the Parliament's proposal simply built on this idea.

[153] See n. 110.

[154] There is also another issue, which needs consideration: the account holder's email data may well include the data of yet other persons, European or otherwise.

[155] See n. 3.

Currently available technologies can be brought to bear, for example controls within networking infrastructure, improving the trustworthiness of the cloud software stack, and security technologies such as authentication, authorisation, encryption, monitoring and audit, so that in some situations "virtual jurisdiction" may be an alternative, and we suggest better, solution than restricting the physical location of data. In addition, we believe Information Flow Control (IFC) shows potential to address some of the problems raised here. Cloud deployment of IFC has not previously been investigated and this is under way in our project.[156]

Our technical work aims at increasing transparency and control for cloud customers, to enable customer trust in cloud providers to be enhanced, and to ease provider compliance. But that alone will not be enough. In the battle for governmental control of access to digital data, users and services providers, of not just cloud computing but more broadly the Internet, are being caught in the middle. There is a pressing need for governments to act in good faith to seek to resolve these problems in a workable and technologically-neutral manner.

[156] See n. 2.

Appendix - Note on “jurisdiction” and Europe-only cloud

The legal concept of jurisdiction is a slippery one. Even lawyers regularly misuse the term or, in order not to mislead their legal audience, have to qualify it with descriptors such as “effective”, “de facto” or “theoretical”. Non-lawyers are almost universally mystified by it.

The purpose of this Appendix is to attempt to reduce some of that mystery and confusion, particularly for a non-legal audience.

1. Persons not things

Law attempts to regulate social relations. Thus it only imposes obligations on persons, including legal persons such as corporations. It is incorrect and thus confusing to state that a law “applies” to a thing, such as the internet or a cloud service, or that a state asserts jurisdiction over that thing. In every case, the law will impose duties and/or confer rights on some person, such as the provider of a cloud service or its user. The days when animals or inanimate objects were subject to court proceedings, usually for causing the death of a person, are long past.

2. Private disputes

Where there is a dispute between two persons which is to be resolved by legal means, the first question is which court should decide the dispute. This is the most common usage of the term “jurisdiction”. If one of the disputants applies to Court A, and the other to Court B, the courts have to decide which of them should hear the dispute. This can happen even within the same state, but is a particular issue when the courts are located in different states. Each court will apply its own rules to decide the matter, and will either take jurisdiction over the dispute or decline jurisdiction. Usually, but not universally, the courts of each state respect the courts of other states, and so if Court A has already decided to take jurisdiction (applying its own rules properly) then Court B will decline to do so, even if its rules would permit it to take jurisdiction.

This is, of course, not directly relevant to the question of a Europe-only cloud. But it does have indirect relevance because courts have the power to order the production of evidence, and this is routine in common-law jurisdictions. Thus if in our example Court A were a US court, it might well order production of data held in a Europe-only cloud service if that data were relevant to deciding the dispute. The person to whom that order was addressed, who might be a party to the dispute or even a complete outsider, such as a cloud service provider, would be in contempt of court if they failed to provide the data. The fact that doing so would be in breach of the law of a European state might not be sufficient as a defence.

3. State regulation

States always have jurisdiction to regulate persons who are physically present in their territory (confusingly, this is often referred to as their “jurisdiction”, using the term in a geographical sense). Their right to do this is rarely contested by other states.

However, it is increasingly common for states to draft their laws so that as worded they apply to persons who are outside their territory – in the context of a Europe-only cloud, data protection laws are a very clear example. Quite what such wording achieves depends on a mixture of legal and non-legal elements.

From a purely legal perspective, these laws drafted with extraterritorial effect assert that the state has the right to regulate the specified activities by foreign persons. Unless there are legal limits on the state’s ability to make such an assertion, then as a matter of *that state’s* law, the law in question applies to the foreign person. However, the courts of a different state will not necessarily accept that assertion – a well-known example from the early days of the internet was the private action brought against Yahoo.com in the French courts for contravening the law against promoting Nazism by allowing Nazi memorabilia to be advertised on the yahoo.com website. The French courts decided against Yahoo, but a Californian court issued a judgment that the French court order could not be enforced against Yahoo by the US courts (though note that this judgment was overturned on appeal on the sole ground that no enforcement threat had yet been made, an example of how the courts attempt to maintain respect for each other's decisions where possible).

There are few limits on a state's power to draft laws with extraterritorial effect. International law contains the principle of comity, under which a state should not attempt to regulate an activity where the law of a different state would more appropriately control it. But there is an exception to this principle if the foreign activity has effect in the state, and as online activities tend to have global effects the principle does little to constrain lawmaking. In any event, the sanction for breach of this principle is no more than the disapproval of other states, which turns the matter from a legal into a political issue.

The main international law limits on making laws with extraterritorial effect come from international treaties, under which states accept obligations to other states. In most cases there are no sanctions for non-compliance, but the benefits of the treaty are sufficient to deter states from passing contradictory law – the international intellectual property treaties are prime examples. One treaty which does contain a sanctions regime is the WTO Treaty, and in the online context Antigua has secured a judgment against the US on the basis that the US laws constraining online gambling are in breach of the treaty's free trade provisions (but it should be noted that the US has not changed its law as a result of the judgment). Any law mandating the use of a Europe-only cloud would be at risk here, to the extent it would exclude non-European providers from the European market.

States may also be subject to their own limits on extraterritorial lawmaking. For example, the US constitution contains two "due process" clauses, and a law which subjected foreigners to US law in contravention of those clauses might well be struck down as unconstitutional. A more likely limit, which would exist even in states without constitutional constraints, is restrictive interpretation of the law by the courts. A UK court has held that online use of a UK-registered trade mark does not infringe UK law if there is no attempt to sell goods or services to persons in the UK. A US court could use the due process provisions of the constitution to decide that it was unable to hear a prosecution of a foreign person, even if on the wording of the relevant law that foreign person had not complied with it.

The final constraint on extraterritorial lawmaking is the state's ability to enforce its law against foreign persons. This depends on such matters as extradition treaties, or the recognition of its national judgments in foreign courts.

The consequence of all this is that it is rarely possible to give a straight answer to the question, "Does European state X have jurisdiction over a cloud service provider/user in non-European state Y?" Only if state X's law is unlawful under its own law or constitution can we answer "No". If the provider/user has assets or staff in state X against which enforcement action can be taken, the answer is clearly "Yes".

Otherwise we are looking at matters of realpolitik, economics and business strategy, and the answers will depend on the players involved. A small business user with no future plans involving European state X might choose to ignore the law completely. A medium-sized player with ambitions to expand its business into Europe might choose to comply, even though currently state X has no means to enforce its law against that player. A global online business might treat the law as a starting point for negotiation, because of its market power within Europe and (perhaps) because its own state will exert political pressure on its behalf. Google has effectively been negotiating with the EU for years with respect to data protection law, though the discussion is couched in terms of what the law actually means rather than whether Google agrees with its content or will comply with the law. It is even arguable that Google's response to the recent *Google Spain* judgment,[157] giving data subjects the right to have some search entries removed from searches, has been crafted as a negotiating tool rather than a simple compliance mechanism. We certainly can't give a straight "Yes" or "No" answer here.

[157] N 58.