An EU-Only Cloud?  
Background Discussion Paper

# Background

## Introduction

This paper provides the background and outlines key legal aspects. Our companion discussion paper, *Cloud Governance [and the EU-only Cloud]*,[[1]](#footnote-1) covers the key technical aspects.

Following Edward Snowden’s revelations of mass surveillance and data collection/interception by US National Security Agency (NSA) and other national security/intelligence agencies, there have been calls for an EU-only cloud, also referred to as the “Schengen cloud” or “Schengen Internet”,[[2]](#footnote-2) apparently involving constraints on the routing of data (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).

In August 2013, German telecommunications provider Deutsche Telekom (DT),[[3]](#footnote-3) with United Internet (who together provide about 2/3 of all German email addresses), announced[[4]](#footnote-4) an "E-mail made in Germany" initiative[[5]](#footnote-5) that would employ only “secure data centers in Germany” for email traffic and use SSL encryption in transmission,[[6]](#footnote-6) thereby (according to United Internet’s head) making it “impossible for any ‘foreign jurisdictions’ to gain access”.[[7]](#footnote-7) Reportedly they would avoid routing such traffic through US hosted infrastructure.[[8]](#footnote-8) However, this initiative only applies to emails between the relevant German email services,[[9]](#footnote-9) not eg emails to persons outside Germany,[[10]](#footnote-10) and data at rest on those servers would be unencrypted,[[11]](#footnote-11) leading to suggestions, including by German security experts, that this move represented “marketing” rather than enhanced protection,[[12]](#footnote-12) and would make Internet use more expensive.[[13]](#footnote-13) That month also, Thierry Breton of EU cloud provider Atos (and France’s former Minister of Economy, Finance and Industry) proposed a Schengen system for data.[[14]](#footnote-14) In fact the idea of a kind of digital Schengen area is not new, having been suggested in 2011 by the Council of the EU’s Law Enforcement Working Party (LEWP) in the context of cybercrime.[[15]](#footnote-15)

Subsequently, in October 2013, apparently after a private meeting with the German government,[[16]](#footnote-16) DT declared its aim to agree with other Internet providers that German Internet traffic would be routed only through domestic connections (ie keeping German Internet traffic within German borders),[[17]](#footnote-17) creating a German-only “Internetz”,[[18]](#footnote-18) with the next step being to expand this to the Schengen area.[[19]](#footnote-19) This “national routing” plan would require the commercial cooperation of other such providers including Telefonica and Vodafone,[[20]](#footnote-20) or legislation to compel such cooperation,[[21]](#footnote-21) without which “there is a risk that competitors or users might file lawsuits claiming discrimination or the curtailment of data traffic”.[[22]](#footnote-22) 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,[[23]](#footnote-24) and it has been suggested that DT’s proposal was “a public relations move”,[[24]](#footnote-25) or even for political gain or to increase DT revenue.[[25]](#footnote-26) Reportedly 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.”[[26]](#footnote-27)

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”; reportedly, Hollande’s office agreed with the proposals and emphasised the importance of a joint initiative.[[27]](#footnote-28) Merkel was not proposing “a European internet” 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”.[[28]](#footnote-29)

If these proposals are to progress, what exactly would an “EU-only cloud” or national cloud entail, how if at all could it be achieved technically and legally, and what would be the consequences?[[29]](#footnote-30) There seem to be two main possibilities regarding the use of any “EU-only cloud” that is created: require use of only the “EU-only cloud”, and no other cloud services; or, allow users the choice of whether to use the “EU-only cloud” or not. Either way, some reliable but flexible method of assuring users that a particular service or provider falls with the “EU-only cloud” category would also be needed, such as certifications or seals.[[30]](#footnote-31)

This paper seeks to lay the foundation for considering the technical and legal feasibility and implications of an EU-only cloud, which is one of the key areas that the MCCRC will be researching. But first, we outline the policy objectives that may underlie the EU-only cloud proposals.

## Policy issues – why an EU-only cloud?

An EU-only cloud approach may seek to meet a range of policy objectives. A chief explicit objective is to prevent unmediated access to EU data by foreign law enforcement authorities (LEAs). Another objective might be to encourage domestic cloud providers and develop domestic infrastructure, which others might term economic protectionism or state aid. One oft-avowed objective is to protect 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 EU users and the development of a single digital market for cloud computing in the EU,[[31]](#footnote-32) which some might consider they would be more willing to do if they had more confidence that their data would be protected, ie based on users’ perceptions of cloud computing and security including LEA access.

While some drivers behind policy objectives may be expressly stated, others may remain undeclared. For instance, in relation to the promotion of EU-only cloud, DT’s declared driver is the protection of German citizens’ privacy, but it may clearly be seeking commercial advantage over its US rivals. While a declared driver of many countries is the restriction of foreign LEA access, an undeclared driver may be the facilitation of access by the country’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 an EU-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.[[32]](#footnote-33) 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 EU country seem 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 the EU and the US on a proposed Transatlantic Trade and Investment Partnership (TTIP), to pressurise the US to adopt stronger privacy laws,[[33]](#footnote-34) while refusing to include data protection in the trade talks.[[34]](#footnote-35)

It is therefore important, when considering the meaning, scope, implementation and implications of “EU-only cloud”, to bear in mind the key underlying policy objectives, and to address how they may be achieved and balanced as appropriate.

Before the issues can be discussed in detail, however, it is important to clarify what exactly is meant by an “EU-only cloud”. We will therefore now analyse the key constituent concepts in the following, slightly different, order

* Cloud
* EU
* Only.

# “Cloud”

“Cloud computing” involves many different types of services, and a one-size-fits-all approach should not be taken to the cloud.[[35]](#footnote-36) When “EU-only cloud” is discussed, what service model is intended to be encompassed: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS),[[36]](#footnote-37) 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. For example, one popular use of IaaS/PaaS is for hosting websites, particularly among organisations that have used cloud for over 18 months.[[37]](#footnote-38) Many websites, including websites of EU-incorporated organisations, are hosted using IaaS/PaaS provided by non-EU, typically US, cloud providers. A blanket prohibition on using non-EU IaaS/PaaS would also ban their use for hosting websites, which seems to cast the net very wide. Surely any requirements regarding “EU-only cloud” ought to take into account the *purpose* pursued by the underlying policy objective (eg to prevent unmediated access by US law enforcement agencies (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 EU-only routing and storage, has been described as “a drastic move according to experts that has not yet been pushed by German leaders”, but has been pursued by other nations, such as Indonesia[[38]](#footnote-39) and Russia.[[39]](#footnote-40)

Even if it is possible for the EU to build IaaS / PaaS services that are “EU-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: eg Facebook, Yahoo! Mail, Microsoft Office 365, Google Apps, YouTube and Dropbox, and “if you're using their services, a national routing system or sandbox will not help.”[[40]](#footnote-41) Again, it does not seem realistic to ban EU users from using Facebook etc, and this may have trade law implications. If Europeans are to be restricted to using EU-only SaaS, must Europe produce homegrown EU equivalents of Facebook, Twitter etc (as well as IaaS/PaaS services)?[[41]](#footnote-42) If so, how can this be achieved?[[42]](#footnote-43)

Also, it should be noted that there are ways for non-EU persons to collect and access information about EU persons other than through their use of cloud computing. In other words, there is a question regarding “EU-only *Internet*”, not just “EU-only cloud”. Many websites, both EU and non-EU, 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 EU users from visiting such websites altogether, which furthermore would again have trade implications. Even when visiting *EU* websites, users may be unable to avoid non-EU routing of material automatically downloaded to their computers when visiting the website, because many EU webpages may be hosted on servers located outside the EU,[[43]](#footnote-44) and/or may incorporate scripts or content from US providers which will accordingly be routed via the US or other non-EU infrastructure, eg the Facebook Like button, which enables Facebook to track users even when not logged in to Facebook at the time.[[44]](#footnote-45) This is but one aspect of a major limitation, to be discussed further below, to the “EU-only cloud” concept, which arises whenever *any* non-EU service, hardware etc is included in the service supply chain.

# “EU”

What is meant by “EU”, in the context of “EU-only cloud”? At first sight the answer might seem obvious, but in fact there are several possibilities here:

* Use only EU cloud providers?
* Confine physical location of data to the EU?
* Process data in accordance with EU laws?

We will suggest that a key underlying issue, which we will return to, 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 country may claim that its courts have jurisdiction to hear certain issues, and may claim jurisdiction to apply its laws to certain situations, sometimes even extraterritorially. Courts of a country 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 country to their contract. Many complex issues are raised by conflicts of laws, in situations where multiple countries could have jurisdiction or multiple laws could apply.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 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.

## Only EU providers?

Could an EU-only cloud entail using the services of EU 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”.[[45]](#footnote-46)

If only “EU cloud providers” should be used, which organisations should (or should not) be considered to be “EU cloud providers” for this purpose. For example, should it only cover organisations incorporated under the laws of an EU Member State? Requiring use of EU-incorporated providers only would need to be reconciled with international trade law obligations.

Also, what about EU-incorporated organisations that are controlled by non-EU parents, eg EU subsidiaries of US technology corporations? Would they be considered to be EU cloud providers, or not? Would organisations incorporated outside the EU, but which have physical operations in the EU, eg branch offices, be considered “EU” for this purpose?[[46]](#footnote-47)

Furthermore, often multiple organisations are involved in the supply chain for a single service, eg providers of sub-services and/or of hardware or software used in providing the service. Are organisations considered to be “EU cloud providers” only if *all* the sub-providers, that they use to provide their services are “EU providers” only too?[[47]](#footnote-48) For example, where a SaaS service is built on a PaaS or IaaS service, must the PaaS/IaaS provider be EU-incorporated also (assuming EU incorporation as the requirement)? How far down the supply chain is it necessary to look? Must even the operator of the data centre used by the PaaS/IaaS provider (if a separate organisation) be EU-incorporated?

What about telecommunications/connectivity 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.[[48]](#footnote-49) Clearly the concern here is that a country with legal jurisdiction over the non-EU provider, eg the USA in the case of US providers, may compel the provider to disclose data to which the provider has access through its provision of the service.[[49]](#footnote-50) Also, routing constraints would be implemented at the telecommunications provider, communications infrastructure, level, not at the SaaS, PaaS or even IaaS level, so telecommunications providers will have a critical role to play in any EU-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.[[50]](#footnote-51) Again one concern is that a country 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[[51]](#footnote-52) concerned. Reportedly Russia has ordered or recommended government agencies in various local regions to stop using Google “and other foreign” services “to heighten ‘information security’”, and “is preparing amendments to legislation that will require Russian companies with state involvement to replace foreign software and IT with Russian products”, with moves to develop Russian-made microchips, satellites and tablets running on a Russian operating system; an order has even been signed that “telecommunications, communications, positioning systems, cartography and similar things should all be produced in Russia”.[[52]](#footnote-53)

***Possible research*** ***being considered by MCCRC*** involves mapping some existing chains and providers/suppliers of cloud services, to provide concrete examples of their typical components and structure, and identities/nationalities of sub-providers involved.

Requiring *all* cloud services, hardware and software etc to be sourced only from EU providers, and no others, may well be difficult to achieve in practice, given that many technology services and hardware/software are operated, supplied or made by non-EU organisations, and any such requirement could also have public procurement law and trade law implications. Furthermore, this would not guarantee that there can be no access from outside the EU to data handled, as even *EU*-produced services, hardware or software may contain unintended vulnerabilities, allowing access by hackers (who may indeed be LEAs) whether from inside or outside the EU; and also EU authorities may choose to communicate EU data to foreign authorities.[[53]](#footnote-54) The policy document *Establishing a Trusted Cloud for Europe*,[[54]](#footnote-55) by the European Commission’s European Cloud Partnership Steering Board, expressed a clear view on this issue:[[55]](#footnote-56)

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 suggests strongly that they 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[[56]](#footnote-57) against them. In other words, this suggests their view is that EU cloud users should use cloud providers who comply with EU laws, whether because they are legally subject to EU jurisdiction, or (it seems) because they *voluntarily choose* to comply with EU laws.

One way may be through adherence to the proposed Code of Conduct for Cloud Computing [providers] prepared by the Commission in association with various stakeholders in the Cloud Select Industry Group (C-SIG), whose draft is being discussed with EU data protection regulators (Article 29 Working Party).[[57]](#footnote-58) ***Proposed MCCRC research*** will include analysis of this Code.

## EU physical location?[[58]](#footnote-59)

Another possibility is that “EU-only cloud” simply means that cloud-processed data must be *physically located* in the EU. This would be consistent with a common approach to “legacy” laws (or their interpretation), that focuses mainly, even exclusively, on the physical location of data. Notably, the EU Data Protection Directive (DPD) restricts the “transfer” of personal data outside the EU, absent “adequate protection” or exceptions or derogations permitted by the DPD. “Transfer” was undefined but 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),[[59]](#footnote-60) whether by transmission of data to a “third country” outside the EEA, remote access to such data from a third country, or physical transportation of hardware storing such data to a third country. 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, eg IBM's patent on controlling data location[[60]](#footnote-61) (and see our companion discussion paper regarding information flow control).

Usually, this location is taken to mean, at least, 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.[[61]](#footnote-62) But what does that mean: the countries of incorporation of such providers? Or countries where they have places of business or operations (which could be different from the country of incorporation, and indeed may be multiple for providers who have operations in several countries)? 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 countries of incorporation/operations etc), 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, countries of incorporation, etc?

Also, 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, for storage of and operations on *indexes* of stored data and other metadata; and for caches eg content delivery networks / edge locations. Indeed, what about the physical location of fibre-optic cables used to transmit data between data centres, and between data centre and customer (or cloud provider staff)?[[62]](#footnote-63) As we now know, intelligence agencies have intercepted communications through access to physical locations through which cables pass, whether in the USA[[63]](#footnote-64) or outside.

This highlights one reason for the fixation on physical location: it’s assumed that physical location will enable intelligible data to be accessed by whoever has access to that physical location, *and* by countries 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 data, whether in persistent storage or in transmission, may be encrypted Thus, encryption may defeat or hinder access to intelligible data regardless of physical data location. Encryption is covered further in our companion discussion paper, but we highlight for now that essentially encrypted data would be intelligible to anyone who can access the relevant decryption keys, but should be unintelligible to others. EEA data protection authorities consider that "encrypted data" remain "personal data",[[64]](#footnote-66) 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).[[65]](#footnote-67)

Communications links may also be encrypted, as Google hastened to do for links *between* its internal data centres soon after the relevant NSA revelations.[[66]](#footnote-68) Encrypted links using Transport Layer Security (TLS), eg https connections in web browsers, is increasingly recommended – and perhaps becoming the norm, so that 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 EU-based or, for example, US-based.

Furthermore, data physically stored in the EU may be accessed remotely (eg over the Internet). Therefore, a focus on “location” could involve multiple locations here too – eg, the country where the person who accessed data was physically located at the time of the access; even the country 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, remote access to personal data physically stored in the EU, by someone then physically located outside the EU, is generally treated in practice as a “transfer” of that data to a location outside the EU. Such remote access could be by an authorised person, but it could also be unlawful, eg criminal hacking. But whether data physically stored in the EU (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 the EU 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 (covered in more detail in our companion discussion paper) 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 of it, rather than as an end in itself.[[67]](#footnote-69) 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 (eg data location) and underlying functional requirements (eg security and accessibility) that could serve as acceptable substitutes.[[68]](#footnote-70)

***For this reason MCCRC's companion discussion paper***[[69]](#footnote-71) summarises technical research aiming to improve governance and control within cloud services (see §5). ***Other proposed MCCRC research*** may include analysis of related initiatives including cybersecurity legislation such as the proposed Network and Information Security (NIS) Directive and eID Regulation, the UK government’s cloud security principles guidance[[70]](#footnote-72) and cyber-essentials and associated certification scheme,[[71]](#footnote-73) the Commission’s SLA standardisation guidance,[[72]](#footnote-74) and the forthcoming ISO27018 standard on a code of practice for cloud providers handling personal data,[[73]](#footnote-75) including ethical dimensions. A sectoral review is planned, to consider cloud security in the financial services industry. As smartphones become ubiquitous and the Internet of Things and “big data” analytics become a reality in cloud computing, MCCRC proposes to research further security and privacy issues in those contexts also.

To recap, physical location of data in the EU is not always necessary or sufficient for ensuring that the data will be protected and handled in accordance with EU laws.[[74]](#footnote-76) 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.[[75]](#footnote-77) Indeed, regarding national data location restrictions, the Trusted Cloud Europe policy document stated:[[76]](#footnote-78)

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 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, ie to ‘oblige internet service companies […] to install and use centres for the storage, management and dissemination of data within the national territory’.[[77]](#footnote-79) 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.[[78]](#footnote-80) When passed in April 2014[[79]](#footnote-81) 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.[[80]](#footnote-82) Widening extraterritoriality appears to be a trend. The UK recently passed The Data Retention and Investigatory Powers Act 2014 (DRIPA),[[81]](#footnote-83) 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,[[82]](#footnote-84) amending its personal data protection law and taking effect from 1 September 2016,[[83]](#footnote-85) 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”,[[84]](#footnote-86) with certain exceptions eg “personal data processing for the purpose of implementation of an international agreement or related Russian law”.[[85]](#footnote-87) The locations of servers hosting such databases must be notified to Roskomnadzor (the Federal Supervision Agency for Information Technologies and Communications).[[86]](#footnote-88) Furthermore, non-compliant services may be added to a “blacklist” register of domain names, network addresses and webpage indexes[[87]](#footnote-89) maintained by Roskomnadzor, and Russian authorities are empowered to require restriction of public Internet access to such services.[[88]](#footnote-90) 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,[[89]](#footnote-91) which would entail establishing data centres in Russia or using Russian data centres with associated costs implications and tight timing even for Russian providers.[[90]](#footnote-92) Practical compliance may also be unclear regarding Russian citizens living outside Russia,[[91]](#footnote-93) 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.[[92]](#footnote-94) More generally, Russia's Association of Electronic Communication (RAEC), a lobbying group for Internet organisations, warned that “many global internet services would be impossible”[[93]](#footnote-95) 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 industry”.[[94]](#footnote-96)

Whether this law would achieve its goals depends on the true nature of those goals, which seem unclear.[[95]](#footnote-97) 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 agencies/LEAs,[[96]](#footnote-98) whereas currently Russia would need to submit mutual legal assistance requests to obtain data from other countries.[[97]](#footnote-99) 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.[[98]](#footnote-100) 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 eg by warrant.[[99]](#footnote-101) Even data stored in Russia, if uploaded, downloaded, or otherwise transmitted over the Internet, may be intercepted by persons from other countries. Which brings us back to the wider Internet physical routing issue.

What are some other possible issues and limitations with physical routing only through a particular nation or region? 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”,[[100]](#footnote-102) or EU-only routing as, “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”.[[101]](#footnote-103)

A fair question to ask is, to what extent *are* European Internet communications actually routed through the USA or otherwise outside the EU, 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.”[[102]](#footnote-104)

***Possible empirical research being considered by MCCRC*** is to update that finding, mapping typical data flows out of and into the EU, including transit.

Other issues include trade law. Current TTIP trade negotiations between the EU and the US have already been mentioned.[[103]](#footnote-105) The Office of the United States Trade Representative opined that Schengen routing “appears to be a means of providing protectionist advantage to EU-based ICT suppliers” and that “any mandatory intra-EU routing may raise questions with respect to compliance with the EU’s trade obligations with respect to Internet-enabled services.”[[104]](#footnote-106) European politicians have reacted negatively, rejecting suggestions of protectionism, and any Schengen cloud may even threaten TTIP.[[105]](#footnote-107)

Mechanisms to restrict physical location of data and/or routing may be feasible technically.[[106]](#footnote-108) 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.[[107]](#footnote-109) However, for national or Schengen *routing* of data, as well as addressing various technical issues,[[108]](#footnote-110) the involvement of multiple Internet providers would be needed, whether through voluntary cooperation or legal compulsion.[[109]](#footnote-111) Also, geographical routing may be somewhat artificial, eg US authorities deliberately routing traffic between US citizens externally outside the USA in order to get round US laws that forbid interception otherwise,[[110]](#footnote-112) and the UK intercepting communications between UK citizens on the basis that they flow through US services and are therefore “external”.[[111]](#footnote-113)

There are also limitations with trying to constrain physical location or routing, as mentioned above regarding emails sent to recipients in another country, or where services or hardware/software used are controlled by providers (including certificate authorities) who are subject to foreign jurisdictions,[[112]](#footnote-114) 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 countries.”[[113]](#footnote-115) 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 “in order to access your data while abroad, you will have to go over foreign networks”.[[114]](#footnote-116)

Furthermore, if the objective of confining physical location and routing of data to the EU is to prevent foreign authorities from accessing such data,[[115]](#footnote-117) that objective will be undermined if *EU* authorities can access such data (as national laws generally allow for national security and/or law enforcement purposes, to varying extents), and choose to pass such data on to foreign authorities.[[116]](#footnote-118) Confining water to a bucket is no good if the bucket’s holder pokes holes in it.

National or Schengen routing proposals have encountered some scepticism, with Pirate Party MEP Amelia Andersdotter terming Friedrich’s proposal “trumped-up lip service… and it's ineffective, and it's hypocritical”, pointing to 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?”, while an expert from Europe’s largest hacker association, German-based Chaos Computer Club, noting 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?”.[[117]](#footnote-119) 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”.[[118]](#footnote-120) Even DT’s outgoing chief executive has acknowledged that “proposing a ‘German internet’ would be like asking for a “German sun.”[[119]](#footnote-121)

Others have expressed concerns about economic as well as openness implications: “If more countries 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”,[[120]](#footnote-122) and “you can create regulations that block off trade in these information services… *[but]* There will be massive sacrifices of economic efficiency”.[[121]](#footnote-123) 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,[[122]](#footnote-124) 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 EU-only cloud might constrain access to non-EU data or services.

Significantly, 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.[[123]](#footnote-125) 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 at the end of the day is beneficial for the citizens”,[[124]](#footnote-126) “The global market cannot be conquered when data is caged within national boundaries and their legal framework”,[[125]](#footnote-127) and “if cloud services are denied scale, they become more expensive. For example, if individual countries work disjointedly on separate national clouds, then the potential is lost.”[[126]](#footnote-128) However, she seems to have cautiously welcomed some aspects of the EU-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”.[[127]](#footnote-129)

## Process under EU laws?

We now discuss another alternative to limiting geographical location or routing – namely, that an “EU-only cloud” means that any processing of “EU data” using cloud computing should take place in compliance with EU laws and principles,[[128]](#footnote-130) *regardless* of the physical locations of data,[[129]](#footnote-131) providers’ or sub-providers’ places of incorporation or operations, etc. This seems to us to be the most technologically-neutral way to address the fundamental underlying concern, and here we use “EU data” simply to mean data that the EU decides should be subject to EU laws:[[130]](#footnote-132) another concept that requires detailed analysis and consideration by policymakers, particularly which data and in what circumstances, eg at least personal data of EU citizens?[[131]](#footnote-133)

A major concern that countries have regarding data is that processing of “their data” (which we use analogously to “EU data”) should be subject to their own laws and jurisdiction. Some countries 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”,[[132]](#footnote-134) illustrating the conflation of physical location with jurisdiction. Unsurprisingly, that approach is rooted in the pre-digital world, where countries 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.[[133]](#footnote-135) 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 *extraterritorially* instead. So, in terms of jurisdiction, countries 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. First, 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*[[134]](#footnote-136)isagain relevant. In that case, 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.[[135]](#footnote-137)

Another feature of digital data that many “legacy” laws do not reflect properly is that (absent copies elsewhere – harder with paper), physical access to a paper file is both necessary and sufficient to access data contained in the file but, as pointed out previously, with *digital* data physical access is neither necessary nor sufficient for access to intelligible data, given remote access and the availability of encryption. This is the point flagged previously regarding laws’ conflation of physical location with access.

With digital data, in practice what matters more than the data’s physical location is *control of access to intelligible data*, which means control of access both to the encrypted data and the relevant decryption keys (as flagged previously). If a country has effective[[136]](#footnote-138) 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 country’s authorities, made to persons incorporated or doing business in that country (or otherwise under its jurisdiction), for data physically located elsewhere but to which the person has intelligible access.[[137]](#footnote-139) It certainly underlies ongoing concerns that US authorities may obtain EU 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, eg such access could be excluded by customers encrypting data securely before upload to the cloud (and managing the keys securely) – please see the companion discussion paper.

All this suggests a different possible approach. The EU could seek to apply EU laws to certain data, not by constraining the data’s physical location to EU territory, but by requiring that only those who are subject to EU jurisdiction may have *access* to that data, especially in intelligible form. Although commercial motivations may have hindered their adoption in practice,[[138]](#footnote-140) such access restrictions may be implemented through technical measures. This approach seems the most promising, in our view. As such, ***MCCRC research*** accordingly includes the use of Information Flow Control (IFC) techniques to enable data and context-specific requirements to control data access and continuously control data flows according to application-level policy. In outline, all data can be tagged to indicate not only ownership but also type (e.g. medical, company, personal), state (encrypted, anonymised, user-input), location and jurisdiction. We are designing, developing and implementing a prototype[[139]](#footnote-141) - this is motivated and presented in our companion discussion paper. And of course, 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.

To summarise, two major issues with digital data are:

* Some persons control, and are authorised to control, access to intelligible data (wherever physically located, eg via remote access) – but they may misuse data and/or disclose data to unauthorised persons, such as cloud providers to foreign governmental authorities; and
* Other persons are *not* authorised to access intelligible data, such as cybercriminals or foreign governmental authorities[[140]](#footnote-143) – but they may nevertheless do so and misuse data, and/or disclose data to unauthorised persons.

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, 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 – see our companion discussion paper.

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

# “Only”

We now come to the “only” of “EU-only cloud”, which we believe is 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 EU laws – but, in today’s globalised world, they may not be subject *only* to EU laws, particularly when digital data are involved. Even EU organisations, particularly those that operate multinationally, may be subject to the laws of several countries simultaneously (including, if they operate in more than one EU Member State, laws of multiple EU Member States, which themselves are not harmonised and may conflict). Similarly, if a non-EU multinational organisation uses “EU-only cloud” services, it would also be subject to multiple jurisdictions.

When different countries claim jurisdiction over an organisation and, more specifically, its data processing, and complying with one country’s demands would break the laws of another country, the organisation is in the invidious position of having to decide which country’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.[[141]](#footnote-144)

But how do organisations choose which country’s laws to break, in practice? A major factor is the type and level of sanctions involved, eg jail in one country vs merely fines in another. This results in a “sanctions arms race” of sorts, as countries continue to change the balance of sanctions, for 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.[[142]](#footnote-145)

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 countries should be able to claim extraterritorial jurisdiction, and limits, transparency and accountability regarding mass surveillance of their own and other citizens’ data. Although the need for such agreement seems widely-acknowledged,[[143]](#footnote-146) the jurisdictional situation is complicated by countries increasingly attempting to extend their jurisdictions extraterritorially,[[144]](#footnote-147) and even specifically prohibiting organisations from complying with other countries’ laws.[[145]](#footnote-148)

How countries eventually find a way to reconcile jurisdictional conflicts is beyond the scope of the MCCRC project. However, we venture to suggest that it is worth considering whether, in relation to digital data, 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 (eg the data subjects, in the case of personal data). In the Microsoft warrant case, 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 an EU Member State?[[146]](#footnote-149) Might that not be a better and more stable determinant of whether the demand impinges on Irish jurisdiction, than the physical location of data?

# Summary of technical and legal/regulatory issues

Our companion discussion paper summarises the technical issues relevant to an EU-only cloud proposal. 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 "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) has the potential to solve some of the problems raised here. Cloud deployment of IFC has not previously been investigated and this is underway in our project.

As regards the key legal and regulatory issues raised by the EU-only cloud proposals, jurisdictional conflicts and extra-territoriality 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*-EU trade, competition law and the free movement of services within the EU, particularly if a Schengen cloud or Internet is intended to exclude the UK and Ireland.[[147]](#footnote-150) 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. EU Member States may have not only multilateral but also bilateral trade commitments.

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 EU-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 EU-only cloud.

All the above issues will be considered as potential topics for further research by MCCRC.

# Concluding remarks

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

1. MCCRC. *Cloud Governance [and the EU-only Cloud]*, *Discussion Paper*. (2014) [↑](#footnote-ref-1)
2. Within the Schengen area, EU citizens may cross country borders freely without being subjected to border checks. This area encompasses all EU Member States *except* the UK and Ireland. It does not include non-EU EEA countries (Iceland, Liechtenstein, Norway) or Switzerland. <http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm> It is therefore unclear whether the UK and Ireland would be excluded from this planned network. [↑](#footnote-ref-2)
3. Which is 32% owned by the German government - <http://www.reuters.com/article/2013/10/25/us-usa-spying-germany-idUSBRE99O09S20131025> [↑](#footnote-ref-3)
4. <http://www.telekom.com/media/company/192834> [↑](#footnote-ref-4)
5. <http://www.e-mail-made-in-germany.de/> and see <http://www.telekom.com/media/company/192834> press release. [↑](#footnote-ref-5)
6. N 3 quoting Oxford Internet Institute expert Professor Ian Brown. [↑](#footnote-ref-6)
7. <http://www.dw.de/german-companies-to-automatically-encrypt-customers-emails/a-17010661> [↑](#footnote-ref-7)
8. <http://www.telecoms.com/170312/deutsche-telekom-avoids-us-servers-another-secure-email-shuts/> [↑](#footnote-ref-8)
9. <http://www.zdnet.com/deutsche-telekom-and-united-internet-launch-made-in-germany-email-in-response-to-prism-7000019266/> [↑](#footnote-ref-9)
10. <http://www.dw.de/germany-looks-to-erect-it-barrier/a-17203480> [↑](#footnote-ref-10)
11. Third party access to such data would be granted “only in compliance with German law” (n 7). 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> [↑](#footnote-ref-11)
12. <http://arstechnica.com/business/2013/08/crypto-experts-blast-german-e-mail-providers-secure-data-storage-claim/> and n 18.

    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> [↑](#footnote-ref-12)
13. “…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>. [↑](#footnote-ref-13)
14. <http://www.europe1.fr/Economie/Breton-creer-une-sorte-de-Schengen-des-donnees-1620759/>. [↑](#footnote-ref-14)
15. “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, eg <http://www.techweekeurope.co.uk/news/eu-proposes-continental-wide-great-firewall-27834>. [↑](#footnote-ref-15)
16. <http://gigaom.com/2013/10/14/why-keeping-internet-traffic-within-borders-is-a-tall-order/> and <http://www.technewsworld.com/story/79286.html> [↑](#footnote-ref-16)
17. “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> [↑](#footnote-ref-17)
18. <http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spying-a-933013.html> [↑](#footnote-ref-18)
19. N 2. [↑](#footnote-ref-19)
20. <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 Dtproposal (n 2). [↑](#footnote-ref-20)
21. “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 2). [↑](#footnote-ref-21)
22. N 18. [↑](#footnote-ref-22)
23. <http://www.wiwo.de/unternehmen/it/spionage-schutz-telekom-will-innerdeutschen-internetverkehr-uebers-ausland-stoppen/8919692.html> [↑](#footnote-ref-24)
24. N 2. [↑](#footnote-ref-25)
25. <http://www.technewsworld.com/story/79286.html> [↑](#footnote-ref-26)
26. N 10 and <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>. [↑](#footnote-ref-27)
27. <http://www.reuters.com/article/2014/02/15/us-germany-france-idUSBREA1E0IG20140215>. [↑](#footnote-ref-28)
28. <http://www.euractiv.com/infosociety/merkel-hollande-lay-foundation-p-news-533560>. [↑](#footnote-ref-29)
29. As the issues are largely similar, in this paper we discuss only “EU-only cloud”, but much of the analysis will apply to a “German-only cloud” or other national cloud. [↑](#footnote-ref-30)
30. See <http://ssrn.com/abstract=2441182>, 2.4, and <http://ssrn.com/abstract=2405971>, 4.10.2, and n 70 pgs 5, 12. [↑](#footnote-ref-31)
31. Eg the Trusted Cloud for Europe initiative (n 55). [↑](#footnote-ref-32)
32. Ibid. [↑](#footnote-ref-33)
33. 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> [↑](#footnote-ref-34)
34. Eg <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>. [↑](#footnote-ref-35)
35. 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 page 3. See chapters 1 and 2 of that book for a more detailed explanation. [↑](#footnote-ref-36)
36. See our companion paper: Cloud Governance, Technical Discussion Paper [↑](#footnote-ref-37)
37. <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/> [↑](#footnote-ref-38)
38. Regulation No. 82 of 2012 regarding the Implementation of Electronic Systems and Electronic Transactions. [↑](#footnote-ref-39)
39. N 2 and <http://www.techweekeurope.co.uk/news/deutsche-telekom-german-internet-nsa-prism-130450> and <http://www.techweekeurope.co.uk/news/deutsche-telekom-test-clean-pipe-135510> [↑](#footnote-ref-40)
40. N 36. Also: “It would not work when Germans surf on websites hosted on servers abroad, such as social network Facebook or search engine Google” (n 3). This could include servers elsewhere in the EU 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). [↑](#footnote-ref-41)
41. Eg “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/> [↑](#footnote-ref-42)
42. “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” – Meyer (n16). Perhaps the Commission’s proposals to enable the EU to recognise the potential of big data may help bring this about, eg 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> [↑](#footnote-ref-43)
43. N 3. [↑](#footnote-ref-44)
44. 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 42). [↑](#footnote-ref-45)
45. <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>. [↑](#footnote-ref-46)
46. The Court of Justice of the EU in the *Google Spain* case ([ECLI:EU:C:2014:317](http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=134919)) 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. [↑](#footnote-ref-47)
47. 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 36) chapter 8. [↑](#footnote-ref-48)
48. <http://www.bbc.co.uk/news/business-28047877> German Interior Ministry spokesman Tobias Plate said: "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 104 regarding US organisation Level 3. [↑](#footnote-ref-49)
49. Although see eg 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>. [↑](#footnote-ref-50)
50. 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 18).

    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” <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> [↑](#footnote-ref-51)
51. 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 guidance<http://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 #7](http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf%20#7) and see further <http://www.nist.gov/director/vcat/cryptographic-standards-guidelines-process.cfm>. [↑](#footnote-ref-52)
52. <http://www.techweekeurope.co.uk/news/russia-wants-domestic-alternatives-replace-foreign-tech-148889> [↑](#footnote-ref-53)
53. See eg n 27: “The NSA can reach information even if it is contained exclusively within Germany, said one former U.S. intelligence official”, n 11 on German intelligence agencies, <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 . [↑](#footnote-ref-54)
54. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935> [↑](#footnote-ref-55)
55. 60% of respondents to the Trusted Cloud Europe survey agreed with the first sentence, nearly 75% with the second – n 70 pgs 7-8. [↑](#footnote-ref-56)
56. It is unclear whether this refers to theoretical or practical enforcement. A country 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 country (eg incorporation there, or assets there), it may have difficulty enforcing against those persons in practice. See further paragraph containing n 136. [↑](#footnote-ref-57)
57. <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140612_wp29_press_release_96th_plenary.pdf> [↑](#footnote-ref-58)
58. For more detailed explication see <http://www.scl.org/site.aspx?i=ed35439>. [↑](#footnote-ref-59)
59. The EEA is the EU plus Iceland, Liechtenstein and Norway. [↑](#footnote-ref-60)
60. <http://www-03.ibm.com/press/uk/en/pressrelease/44563.wss> - although see prior work such as <http://timharris.co.uk/papers/2005-location.pdf>. [↑](#footnote-ref-61)
61. 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>. [↑](#footnote-ref-62)
62. From a DPD perspective, mere transit, ie 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). [↑](#footnote-ref-63)
63. Eg 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> [↑](#footnote-ref-64)
64. N 62. [↑](#footnote-ref-66)
65. Cloud Computing Law (n 36), chapter 7. [↑](#footnote-ref-67)
66. <http://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html> [↑](#footnote-ref-68)
67. W. K. Hon and C. Millard, “How Do Restrictions on International Data Transfers Work in Clouds?”, in C. Millard, Ed. (n 36) chapter 10, and n 59. [↑](#footnote-ref-69)
68. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=6608> pgs 4-5. [↑](#footnote-ref-70)
69. See our companion discussion paper. [↑](#footnote-ref-71)
70. <https://www.gov.uk/government/publications/cloud-service-security-principles> [↑](#footnote-ref-72)
71. <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> [↑](#footnote-ref-73)
72. <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138> [↑](#footnote-ref-74)
73. <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498> [↑](#footnote-ref-75)
74. N 69 and n 59. [↑](#footnote-ref-76)
75. *Lindqvist* ([ECLI:EU:C:2003:596](http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=230010)) and n 59. [↑](#footnote-ref-77)
76. N 55, 19. [↑](#footnote-ref-78)
77. <http://dataguidance.com/news.asp?id=2129> [↑](#footnote-ref-79)
78. See eg <http://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html> [↑](#footnote-ref-80)
79. <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm> [↑](#footnote-ref-81)
80. 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. [↑](#footnote-ref-82)
81. <http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted/data.htm>/ [↑](#footnote-ref-83)
82. No. 553424-6 <http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=553424-6> [↑](#footnote-ref-84)
83. Reportedly the draft has been signed by Russia’s President Putin and accordingly is now law. <http://www.zdnet.com/putin-signs-data-retention-law-7000031897/> [↑](#footnote-ref-85)
84. <http://en.itar-tass.com/russia/739029> [↑](#footnote-ref-86)
85. <http://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/7/Russias-Internet-Privacy-Act-will-have-wide-implications-for-foreign-companies/> [↑](#footnote-ref-87)
86. N 84 and <http://www.techweekeurope.co.uk/news/russian-government-will-force-companies-store-citizen-data-locally-148560> [↑](#footnote-ref-88)
87. It is unclear how webpage indexes would be registered. [↑](#footnote-ref-89)
88. Nn 86, 87. [↑](#footnote-ref-90)
89. Nn 86, 87. [↑](#footnote-ref-91)
90. 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> and other Internet organisations also consider 2 years is insufficient to find or build Russian data centres (n 85). [↑](#footnote-ref-92)
91. Eg <http://tech.slashdot.org/comments.pl?sid=5365111&cid=47387219> [↑](#footnote-ref-93)
92. <http://www.alrud.com/upload/iblock/3ea/Newsletter_Ban%20to%20store%20personal%20data%20outside%20Russia.pdf> . [↑](#footnote-ref-94)
93. N 85. [↑](#footnote-ref-95)
94. <http://www.cnet.com/uk/news/facebook-gmail-skype-face-russia-ban-under-anti-terror-plan/>. [↑](#footnote-ref-96)
95. Eg <http://techcrunch.com/2014/07/02/russia-moves-to-ban-online-services-that-dont-store-personal-data-in-russia/> [↑](#footnote-ref-97)
96. Eg <http://nakedsecurity.sophos.com/2014/07/04/russias-latest-internet-law-proposal-anti-nsa-or-pro-fsb/>, n 85 and n **Error! Bookmark not defined.**96. And on German-only email routing, see n 13: “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”. [↑](#footnote-ref-98)
97. See I. Walden, “Law Enforcement Access to Data in Clouds”, in C. Millard, Ed. (n 36), chapter 11. [↑](#footnote-ref-99)
98. 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 92). See also n 88, which noted another possible motivation: to encourage development of Russian online services. [↑](#footnote-ref-100)
99. 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 eg <http://www.v3.co.uk/v3-uk/news/2350252/apple-and-cisco-lend-support-to-microsoft-in-cloud-data-access-debate> It lost the appeal, and is being given time to appeal further, which Microsoft has indicated it will do. <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, eg 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> [↑](#footnote-ref-101)
100. Ibid. [↑](#footnote-ref-102)
101. Office of the United States Trade Representative, <http://www.ustr.gov/sites/default/files/2013-14%20-1377Report-final.pdf#5> [↑](#footnote-ref-103)
102. <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 3). 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 still access them, although the company vehemently denies this.” (n 18). [↑](#footnote-ref-104)
103. Paragraph containing n 35. [↑](#footnote-ref-105)
104. N 103. [↑](#footnote-ref-106)
105. <https://www.techdirt.com/articles/20140417/03092626940/german-politicians-hit-back-ustr-criticisms-european-cloud-idea.shtml>. [↑](#footnote-ref-107)
106. Eg 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> [↑](#footnote-ref-108)
107. Eg Heroku <http://gigaom.com/2013/04/25/heroku-comes-to-europe-but-data-protection-issues-remain/> [↑](#footnote-ref-109)
108. Eg “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> [↑](#footnote-ref-110)
109. N 36. “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 3). [↑](#footnote-ref-111)
110. <http://ssrn.com/abstract=2460462> [↑](#footnote-ref-112)
111. <http://www.nytimes.com/2014/06/17/business/international/british-spy-agencies-said-to-assert-broad-power-to-intercept-web-traffic.html> [↑](#footnote-ref-113)
112. Such as foreign social networking services, even EU websites that incorporate scripts or plugins from foreign services - see part 1.2. [↑](#footnote-ref-114)
113. N 18. [↑](#footnote-ref-115)
114. <http://www.dw.de/deutsche-telekom-internet-data-made-in-germany-should-stay-in-germany/a-17165891> [↑](#footnote-ref-116)
115. As stated by a DT spokesman regarding national routing: “Secret services of countries outside this area would then find it much more difficult to access this data traffic” (n 16). Note that he did not say “impossible” – see also n 27: “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”. [↑](#footnote-ref-117)
116. N 54. [↑](#footnote-ref-118)
117. N 27. [↑](#footnote-ref-119)
118. N 3. [↑](#footnote-ref-120)
119. N 42. [↑](#footnote-ref-121)
120. N 2 and <http://www.wired.co.uk/news/archive/2014-02/06/tim-berners-lee-reclaim-the-web> [↑](#footnote-ref-122)
121. <http://www.npr.org/blogs/parallels/2013/10/16/232181204/are-we-moving-to-a-world-with-more-online-surveillance> [↑](#footnote-ref-123)
122. <http://ec.europa.eu/justice/fundamental-rights/charter/>. [↑](#footnote-ref-124)
123. 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. [↑](#footnote-ref-125)
124. <http://www.dw.de/no-welcome-for-deutsche-telekom-national-internet-plans-from-eu-commission/a-17219111> [↑](#footnote-ref-126)
125. N 13. [↑](#footnote-ref-127)
126. N 46. [↑](#footnote-ref-128)
127. <http://gigaom.com/2014/02/17/after-us-squashes-no-spy-hopes-european-leaders-discuss-ways-to-protect-citizens-data/>. [↑](#footnote-ref-129)
128. 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> [↑](#footnote-ref-130)
129. 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) 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, eg 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. [↑](#footnote-ref-131)
130. For example, the Audiovisual Media Services Directive introduces a concept of “European works”, and regulates works falling within that definition. [http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L47474747470013&rid=1](http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L0013&rid=1). [↑](#footnote-ref-132)
131. 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 will be discussed in a forthcoming Cloud Legal Project paper <http://cloudlegalproject.org>. [↑](#footnote-ref-133)
132. <http://www.reuters.com/article/2014/03/19/us-brazil-internet-idUSBREA2I03O20140319>. [↑](#footnote-ref-134)
133. <http://www.scl.org/site.aspx?i=ed35439> text to fn 7-8. [↑](#footnote-ref-135)
134. n 39. [↑](#footnote-ref-136)
135. n 47, paras 55-56. [↑](#footnote-ref-137)
136. Whether jurisdiction claimed by a country is *effectively* enforceable in practice is a different issue, particularly when it attempts to apply its laws extraterritorially (ibid, text to fn 35). Extraterritoriality is discussed further below. [↑](#footnote-ref-138)
137. Such as the US warrants and Brazilian court orders against Microsoft and Google – n 101. [↑](#footnote-ref-139)
138. Eg, 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”. Eg <http://rt.com/usa/163600-google-encryption-tool-nsa/> [↑](#footnote-ref-140)
139. 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>. [↑](#footnote-ref-141)
140. Although foreign LEAs may in some cases be authorised, or they may not require authorisation from the country in which the data resides - see Council of Europe Cybercrime Convention, art 32. [↑](#footnote-ref-143)
141. <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> [↑](#footnote-ref-144)
142. <http://ssrn.com/abstract=2405971>. [↑](#footnote-ref-145)
143. Eg <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> [↑](#footnote-ref-146)
144. Eg Brazil’s solution to not requiring data localisation was wide extraterritoriality. Concerns have been noted eg: “…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, eg 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. [↑](#footnote-ref-147)
145. As with the “anti-FISA” provision introduced by the European Parliament in the draft Data Protection Regulation – n 145. [↑](#footnote-ref-148)
146. There is also another issue, which needs consideration: the account holder’s email data may well include the data of yet other persons, EU or otherwise. [↑](#footnote-ref-149)
147. See n 2. [↑](#footnote-ref-150)