Data Localization Laws and Policy
The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens

W. Kuan Hon, kuan0.com

http://www.e-elgar.com/shop/data-localization-laws-policy
http://www.e-elgar.com/data-localization-laws-and-policy-companion-site

Update/Supplement
As at 1 May 2017

All paragraph and page number references are to paragraphs and pages of the book, unless otherwise stated.

Preface

p.xii – Commission Vice President Andrus Ansip acknowledged in November 2016 that the trend to data localization (in the context of non-personal data) was 'going up' rather than down: so the EU had '50 different rules in 21 member states'. But the trend continues. In November 2016, China passed a law requiring data localization in certain circumstances, whose disadvantages for China have been pointed out.

1. Chapter 1 - Background

1.2.3

p.4-5 – in this connection it is interesting to note an October 2016 opinion by the Bavarian DPA (Germany) on service providers under the GDPR. Such providers may potentially have access to personal data. This opinion suggests that the Bavarian DPA would not treat a provider even as a 'processor' if it only conducts technical maintenance, presumably despite having incidental access to personal data, unless the maintenance was specifically for the purpose of processing personal data. This supports my view that many cloud providers should not be treated as processors simply because they have the technical ability to access personal data processed by customers using their services, unless and until they actually do so.

1.3

p.7, n.18 – AWS launched a London, UK region in December 2016. Microsoft offered Azure backup and site recovery services from its UK datacentres from February 2017.

p.10, first para. last sentence – a package of documents, including a proposed ePrivacy Regulation to update and replace the ePrivacy Directive, was published by the Commission in January 2017. The WP29 issued its opinion on the proposed Regulation, *WP247*, in April 2017. It does not affect data localization in the sense discussed in this book, although it covers device location data.

1.5.1

p.13, first para. - unlike the DPD, the GDPR currently only applies to EU Member States, not other EEA countries. An EEA joint committee decision (see p.1, n.1) would be needed to extend the GDPR to the other EEA countries. As at 1 May 2017, no such decision has yet been made, and it seems unlikely that it will even appear on the joint committee's agenda until autumn 2017 at the earliest.

p.13, n.25 – for example, Germany's draft legislation to implement the GDPR, as at January 2017, contained 'questionable' deviations from the GDPR which were considered 'problematic'; their enforceability is 'not certain'.

p.13, n.26 – on Brexit, the UK Secretary of State for Culture, Media and Sport, Karen Bradley, stated in October 2016 that the UK would be implementing the GDPR notwithstanding Brexit, while the Minister for that department, Matt Hancock, confirmed this in a cyber security review in December 2016, further stating that the GDPR would be 'key to ensuring strong organisational data protection regimes supported by strong cyber security'. In April 2017, the UK launched a consultation on the derogations in the GDPR (which allows for many Member State flexibilities – see 1.5.2, p.13, n.25).

Further on Brexit, see update to 5.2.4, p.160, in this document.

2. Chapter 2 – Legislative history and objectives

2.2.1

p.26, first para – in November 2016, Russian DPA Roskomnadzor took enforcement action against LinkedIn (now owned by Microsoft) and blocked access to it on various grounds, including breach of Russia's data localization law, as LinkedIn's servers were thought to be US-located based on the WHOIS database. However the same month, following an inspection of Microsoft's (separate) Russian subsidiary, Roskomnadzor declared the data localization issue regarding that subsidiary was 'closed'. Further developments on LinkedIn are awaited.

p.26, n.5 – China has introduced a data localization requirement for 'key information infrastructure' under its new network security law, effective from 1 June 2017.

2.2.4

p.32, penultimate para. and n.13 – parties to Convention108 are listed and shown in a map. Four other countries have been invited to accede but have not yet ratified, as 1 May 2017.

In January 2017 the Commission urged third countries to accede to Convention108 and Convention108-AP, as the only binding multilateral instrument covering data protection, and wants to 'actively promote' swift adoption of Convention108's planned update with a view to the EU becoming a party (COM(2017)7 final, p.11-12).

2.2.6

p.35, last para. – in January 2017, the Commission issued a proposed Regulation to update the CIDPR in line with the GDPR, with associated documents. The WP29 issued a statement on the proposed update in April 2017, but did not discuss transfer aspects. Similarly with the EDPS's opinion on the proposal, save that he recommended expanding the EDPS's international cooperation activities to mirror the GDPR's Art.50 (6.4.5, p.258).

p.36, first and second full paras. – an evaluation study of the CIDPR (2015, but published in January 2017) found (its p.139) that because Art.2(g) CIDPR excludes, from the definition of 'recipient', 'authorities which may receive data in the framework of a particular inquiry', some EU institutions/bodies have interpreted Art.9 CIDPR as allowing transfers to such authorities (in this context, any transmissions/disclosures, not just international transfers); however, the EDPS disagrees and considers that the CIDPR's transfer rules apply to such authorities. Also, the evaluation noted that it was unclear whether such authorities were meant to be only EU bodies, authorities subject to the DPD, or even third country authorities.

Similarly, an associated detailed analysis of the CIDPR highlighted this issue (p.6 of the analysis), also noting some uncertainty as to whether a processor should be considered a 'recipient' for transfer purposes; the EDPS considers (ibid) that not treating processors as 'recipients' hinders application of the CIDPR's transfer rules, and that those rules, including international transfer restrictions, do apply to 'transfers' to processors.

The proposed Regulation to update CIDPR follows the GDPR in referring only to transfers 'to a third country or to an international organisation', completely eliminating any mention of transfers to 'recipients'. Perhaps this was partly to address the problems with the definition of 'recipient' outlined above, and partly to mirror the GDPR more closely, but I consider this an unfortunate development given the uncertainty discussed in Chap.2 of the book regarding what is a 'transfer'.

2.2.8

p.38, last para. – in February 2017, Canadian lawmakers began hearing from witnesses on a review regarding possible amendments to PIPEDA, particularly for GDPR 'essential equivalence'. Currently, PIPEDA does not provide for fines, or rights of erasure or data portability.

p.39, last para. – in November 2016, APEC heads of state emphasized the importance of implementing CBPR. In January 2017, South Korea indicated its intent to participate in CBPR, while Chinese Taipei plans to conclude an internal review to join in 2017, and Singapore and the Philippines reportedly also plan to join.

p.40, first para. – the Commission has suggested that ways 'could be explored' to promote convergence between BCRs and CBPRs as regards both their applicable standards and application process (COM(2017)7 final, p.11), and is 'looking forward' to 'further developing' its working relationship with APEC and others to foster a worldwide culture regarding privacy and data protection.

p.40, first full para., first sentence – as at 1 May 2017, there are 20 participating organizations (one Japanese, the rest US). They are listed at https://cbprs.blob.core.windows.net/files/APEC%20CBPR%20Compliance%20Directory_April2017.xlsx – this compliance directory is linked to from the main CBPRS page http://www.cbprs.org/.

p.40, first full para., penultimate sentence – in April 2017 the FTC approved final orders with three of the companies concerned, resolving allegations that they deceived consumers by misrepresenting their participation in CBPR.

2.2.10

p.42, first para. – the CoE has changed the links to the draft protocol and explanatory report but the link to the consolidated text of the proposed modernized Convention108 remains unchanged.

Although the CoE's Secretary-General gave a speech in June 2016, noting that the process would be finalized by governments through the CoE Committee of Ministers, and hoping that the revised Convention108 text would be adopted by the end of 2016, this has not transpired. While public statements on the progress of the modernization are lacking, some information may be gleaned from the CoE's website. A draft report of a March 2017 meeting of the CoE's Committee of Legal Advisors on Public International Law (CAHDI) shed some light on the reasons for the delay: CAHDATA agreed a 'first draft' in June 2017, but 'Afterwards, taking into account that several issues (EU voting rights, national security exceptions, transborder data flows, entry into force) with important political and legal implications beyond the expert level remained pending, the first draft was submitted to the Rapporteur Group on Legal Co-operation (GR-J) of the CoE's Committee of Ministers for examination and decision. The Director pointed out the importance of the outcome of these negotiations for the protection of personal data at the European and international level.'

A September 2016 CM(2016)124 meeting of the bureau of the consultative committee of Convention108 (T-PD) welcomed CAHDATA's finalization of its work on modernizing Convention108 and reaffirmed to the Committee of Ministers its full support for the modernization and Ministers' deputies 'took note' of the meeting report in October 2016. The November/December 2016 T-PD meeting noted information on 'recent developments' at the Committee of Ministers' Rapporteur Group (GR-J) on Legal Co-operation's November/December 2016 meetings. GR-J held informal consultations on the draft amending protocol and explanatory report in January 2017 and March 2017 (and met afterwards in March 2017 and April 2017. T-PD also 'took note' in its March 2017 meeting of information on 'latest discussions' regarding the modernization of Convention108 at the level of GR-J scheduled for April 2017, so it appears that earlier planned meetings of GR-J were not sufficient to reach agreement. On 28 April 2017, the CoE's Parliamentary Assembly adopted a recommendation 2102(2017) Provisional version on Technological convergence, artificial intelligence and human rights, calling on the Committee of Ministers to 'finalise without further delay' the modernization of Convention108. Other GR-J meetings are scheduled for May 2017 and June 2017; although the agenda has not been published for any of those, it seems that at least the June meeting is to discuss the proposed modernization of Convention108.

2.4.4

p.61, first full para., p.63 , first para., and generally – on 'recipients', see the update in this document to 2.2.6, p.36, first full para.

2.4.5

p.63, first full para – on 'recipients', see the update in this document to 2.2.6, p.36, first full para.

2.5

p.68, first para. - worryingly, even some security experts seem to equate location with jurisdiction – see one April 2017 example.

3. Chapter 3 – The 'transfer' concept

3.6.3.1

p.87, first full para., and n.27-28; p.89, first para. – on 'recipients', see the update in this document to 2.2.6, p.36, first full para. On providers not necessarily being 'processors', see update to 1.2.3, p.4-5.

3.7.4.1

p.93, n.36 – for some key documents in the *Microsoft warrant* case, see https://www.unitedstatescourts.org/federal/ca2/14-2985/. A recent article by Tene about the case also argues against laws on data location.

p.93, first full para. – Google too is fighting a similar US warrant cases (see the full text memorandum of decision): *In re Search Warrant No.16-960-M-01 to Google* and *In re Search Warrant No.16-1061-M to Google,* US District Court, Eastern District of Pennsylvania*, Nos. 16-mj-00960, 16-mj-01061*. Some of the main documents are at https://www.unitedstatescourts.org/federal/paed/520550/.

In February 2017, magistrate judge Thomas J. Rueter ordered Google to disclose to the FBI customer emails stored on non-US servers, also following search warrants issued under the SCA for the contents of email communications related to two separate criminal investigations. Google had refused to comply with the warrants as regards data not known to be located in the US, based on the *Microsoft warrant case*.

However, in both these investigations, the account holders were US, unlike in the *Microsoft warrant* case: 'Each account holder resides in the United States, the crimes they are suspected of committing occurred solely in the United States, and the electronic data at issue was exchanged between persons located in the United States', facts which the US Department of Justice emphasized. Judge Rueter noted that, in a concurring opinion (on the *Microsoft warrant* case's 3-judge panel appeal court decision in July 2016), Judge Lynch had ultimately concluded that because the nationality of the Microsoft account holder was unknown and that person was probably a citizen of Ireland, the US Congress did not intend for the SCA 'to reach situations of this kind'. So that was one distinguishing feature and, as I have argued, an important one.

Judge Rueter also noted Judge Lynch's view that it seemed 'at least equally persuasive' that the privacy invasion where the person whose privacy is invaded customarily resides, as opposed to the majority view that the locus of the invasion is 'where the private content is stored'. He ruled that 'When Google produces the electronic data in accordance with the search warrants and the Government views it, the actual invasion of the account holders' privacy - the searches - will occur in the United States. Even though the retrieval of the electronic data by Google from its multiple datacentres abroad has the potential for an invasion of privacy, the actual infringement of privacy occurs at the time of disclosure [to the FBI] in the United States.' Therefore, there was no issue of applying the SCA extra-territorially here, in his view. As for comity, no foreign nation's sovereignty would be interfered with 'in any ascertainable way at the time the two warrants at issue are executed because the searches will be conducted in the United States'.

In terms of data flows, he further considered that 'Electronically transferring data from a server in a foreign country to Google's datacentre in California does not amount to a "seizure" because there is no meaningful interference with the account holder's possessory interest in the user data.' Indeed, according to Google and the government, Google regularly transfers user data from one datacentre to another without the customer's knowledge, and such transfers do not interfere with the customer's access or possessory interest in the user data or, even if it does interfere with the account owner's control over his information, this interference is 'de minimis and temporary'.

This leads to another important distinguishing feature: in the *Microsoft warrant case*, the majority made the key assumption that 'messages stored in the "cloud" have a discernable [sic] physical location'; in that case, Judge Rueter noted, all relevant user data of a presumably Irish citizen was located exclusively in one datacentre in Ireland and remained stable there for a significant period. However, in the case of Google, the same critical assumption could not be made because of the

'changeable and divisible nature of Google's cloud technology', whereby Google's data are stored in a dynamic network which distributes data, 'sometimes in bits and pieces', to servers located in the Americas, Asia and Europe. Google's architecture divides user data among datacentres in different countries, and also partitions user data into shards which could be stored in different locations. Google stated that different parts of a single file may be stored in different locations (and, accordingly, different countries) at the same time, with its state-of-the-art intelligent network that, for some data types (including some of the data at issue), automatically moves data between locations on Google's network as frequently as needed to optimize for performance, reliability, and other efficiencies. As a result, the country or countries where specific user data, or components of data, is located may change, perhaps even between the time legal process is sought and served. This illustrates that not all cloud technologies should be treated in the same way; the WP29 based *WP196* (p.100) on Google's technology, but Microsoft's (and many others') does not necessarily take the same approach, and data location may be much more ascertained under some other providers' technologies. Nevertheless, Google's approach clearly illustrates the difficulties with basing jurisdiction on data location.

Google had argued that it did not currently have the capability, for all of its services, to determine the location of the data and produce that data to a human user at any particular point in time. It produced all records it could ascertain were stored in the US, but would not produce any other data. However, Judge Rueter felt that to adopt Google's interpretation of the Microsoft decision would make it impossible for the Government to obtain the sought-after user data through existing MLAT channels, given the data's unknown and movable location, leading to 'absurd results' (as one commentator, Orin Kerr, noted, because the data location are unknown to Google, which configured its network so that that the data could only be accessed from its Californian HQ, applying reasoning in the Microsoft warrant case would result in that data being 'completely immune from legal process'). In contrast, on Judge Rueter's 'commonsense' interpretation, 'Google will gather the requested undisclosed data on its computers in California, copy the data in California, and send the data to law enforcement agents in the United States, who will then conduct their searches in the United States'. He had noted the US government's argument that Google's architecture created an 'insurmountable obstacle for the Government to overcome in the MLAT process'; given the movability and sharding of Google's data, the US government could never employ established processes such as MLATs to request assistance from another country to access Google's user data stored in that country.

As at 1 May 2017, Google's appeal of the magistrate judge's ruling is still ongoing, where Microsoft, Amazon, Cisco and Apple have filed a joint amici curiae brief in support of Google. Since that Google warrant case, there have been a spate of judges in other US districts, also dismissing concerns about extraterritoriality, ruling that there was no extraterritorial application of the SCA, and ordering disclosure by:

- Yahoo and Google, of data regarding specified email accounts (In re Information associated with one Yahoo email address that is stored at premises controlled by Yahoo, In re Two email accounts stored at Google, Inc., Case Nos.17-M-1234, 17-M-1235, US District Court, Eastern District, Wisconsin, February 2017);
- Yahoo, regarding an email account (*In re premises located at: [redacted]@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc.*, Case No.6:17-mj-1238, US District Court, Middle District of Florida, Orlando Division, Florida, April 2017); and
- Google, regarding certain emails accounts (*In re the search of content that is stored at premises controlled by Google*, Case No.16-mc-80263-LB, US District Court, Northern District of California, San Francisco Division, California, April 2017).

Florida magistrate judge Thomas B. Smith originally followed the *Microsoft warrant case* and limited the scope of the warrant granted so that if Yahoo had relevant information stored at a place outside the United States, it was not required to produce that information. However, he then reconsidered and reversed his ruling, on the basis that the SCA gave courts *in personam* to order providers of electronic communication services to produce information under its control (more like a subpoena), including electronic data stored in the cloud. Following the dissenters in the *Microsoft warrant case* and agreeing with the government that the SCA's focus was compelled disclosure, not privacy, he noted that a court with *in personam power* can require a person to take acts, including compelled disclosure of information, either within or outside of its territorial jurisdiction, because the court's jurisdiction over the person and its compulsion of that person is not extraterritorial, even if the information required to be disclosed is located outside of the US. Accordingly he issued another warrant for the information

sought, not limiting it to the territorial boundaries of the US. The citizenship/location of the account-holder was not stated.

In the Wisconsin case, the targeted Yahoo account holder (with whom a US person communicated) was believed to be a European resident, but there was no indication that the relevant Google email accounts were used by persons outside the US. In both instances, magistrate judge William E. Duffin followed the dissenting judges in the *Microsoft warrant case*, stating that "the relevant section of the SCA is not best regarded as an authorization for law enforcement to seize data but rather as a command for a service provider to disclose data in its possession. If that service provider is subject to the jurisdiction of the court, the court may lawfully order that service provider to disclose, consistent with the SCA, that which it can access and deliver within the United States... It is immaterial where the service provider chooses to store its customer's data; what matters is the location of the service provider... As an order compelling action on the part of service provider, what matters is the location of the service provider. Provided the service provider is within the reach of the court, the court may lawfully order that service provider to disclose data in the service provider's custody and control, without regard of where the service provider might choose to store the ones and zeros that comprise the relevant data.'

Californian magistrate judge Laurel Beeler preferred the views of the dissenters in the *Microsoft warrant case*, stating 'The SCA regulates disclosure of data in a service provider's possession. The service provider — Google — is in the district and is subject to the court's jurisdiction; the warrant is directed to it in the only place where it can access and deliver the information that the government seeks. This disclosure [from Google's US headquarters] is a domestic application of the SCA. The court thus orders Google to produce all content responsive to the search warrant that is retrievable from the United States, regardless of the data's actual location'. The location/citizenship of the account holders concerned was not stated in this case either.

I have covered these cases in detail because they very much highlight the tension between basing jurisdiction on persons versus data location. They make it even more likely that the issue will eventually reach the US Supreme Court, the US's highest judicial arbiter, but that process may well take years. US academic Jennifer Daskal has urged a legislative solution, suggesting (see paper) several options to balance the security, privacy and economic interests concerned, where the data relate to a non-US citizen or resident: allowing warrants for US-controlled data regardless of location but requiring a comity analysis, notice to the non-US government concerned, or reciprocal agreements with other countries based on notice and opportunity to object (and see the summary of the never-passed ICPA, p.94). This ties in with my arguments for a focus on persons over data locations.

p.94, first para. – on Google, see the Google warrant case (update above, p.93, first full para).

3.7.3.5

P.108, n.64 – similarly, Deutsche Telekom's "German cloud" (a public cloud) has reportedly met with strong demand particularly from financial services, local government and SMEs. According to an April 2017 study, UK IT decision makers still prefer storage in the UK, but followed by the US (far ahead of Germany, interestingly). But 54% of IT decision-makers in Germany (14% in the UK) perceived the US 'as an untrustworthy destination'. The 'discomfort factor' about personal data being held outside the EEA is so great that, in April 2017, Photo-Me, the only organisation approved to provide photos for Ireland's online passport application service, had to correct its privacy policy to delete a generic statement about transferring 'personal information' to third countries. It had not been transferring Irish citizens' passport photos in third countries, in any event. While dating from 2015, a previous survey also found that UK lawmakers considered 'offshoring of data' to be the greatest barrier to public sector cloud adoption.

3.7.7.1

p.112, third para. – 'a Communication is expected in 2016 (Commission 2016e)' – in fact a Communication on 'Building a European Data Economy' was issued in early 2017, COM(2017)9 final.

It noted data localization laws, policies and practices in the EU in areas other than personal data, and discussed the free flow of data, but only within the EU and only of non-personal data (emphasizing that the GDPR 'bans restrictions on the free movement of personal data *within* the Union' where based on reasons connected with data protection – ibid. p.5). Furthermore, it sought views rather than making concrete proposals for near-future action on unjustified localization of non-personal data, even within the EU. It therefore seems that any changes are unlikely for some time, particularly given the focus on other proposed legislation like the ePrivacy Regulation (see update in this document to 1.3, p.10, first para. last sentence) and the planned update to the CIDPR (see update in this document to 2.2.6, p.35, last para.).

3.7.7.3

p.114, first full para - US President Trump, soon after taking office, withdrew the US from the Trans-Pacific Partnership negotiations (TPP). While he has not yet officially withdrawn the US from TTIP, many believe that this will be inevitable.

p.114, final para. – to expand on this point, on the one hand the Commission emphasizes that adequacy decisions are *one-way* decisions by the Commission (COM(2017)7 final, p.9, n.42). But, on the other hand, it suggests that such a decision can somehow reduce the risk of the relevant third country relying on data protection to impose 'unjustified data localisation or storage requirements'. This does not seem to make sense, with respect. Even if the Commission has decided that a third country is 'adequate' for EU data protection law purposes, that does not mean that the country is required in turn to decide that it need not require localization (on its own territory) of its own residents' personal data – because the Commission's decision is unilateral, not bilateral. That country may be more favourably inclined towards the EU politically, if it has been declared 'adequate' by the Commission, but just because a third country's laws are deemed to meet EU standards does not necessarily mean that EU laws must or will be deemed by that country to meet its own standards.

3.7.8

p.115, first para. under 3.7.8 – as another possible example of lack of awareness that certain uses may involve transfers outside the EEA, research (highlighted by CNIL) analyzing some 1,500 of the most popularly-used mobile apps in the EEA found that 295 (20%) of the apps analyzed transferred personal data outside the EEA, to 213 non-EEA servers (67% of the servers found to be receiving personal data from the apps were non-EEA) - without any privacy policy, in the case of 108 of those apps.

3.8

p.118, last full para. – the EDPS still interprets 'transfer' in this way (p.61 of evaluation study of CIDPR, from 2015 but only published in 2017).

p.119, first para. – the GDPR prohibits transfers under third country court orders and the like unless the third country uses an MLAT or similar, yet a Belgian court in late 2016 fined Microsoft for not disclosing Skype communications even though the Belgian authorities did not attempt to invoke Belgium's MLAT with Luxembourg.

p.119, last para. - on providers not necessarily being 'processors', see update to 1.2.3, p.4-5.

4. Chapter 4 - Assumptions

4.5.1

p.136, n.13 – see in this document the updates to 5.3.3.4, p.169, n.23.

4.5.1.1.2

p.139, n.22 – on physical risks, more recent research (p.8, fig.4:) indicated about 1500 incidents from hacking, but only about 100 from physical risks, mainly laptop loss/theft.

4.5.1.2.3

p.141 – indeed, under current US laws, US authorities have more powers to access data located outside US soil (particularly under President Reagan's Executive Order 12333), than they have to access data *inside* the US under the US FISA. In January 2017, the US Central Intelligence Agency (CIA) announced updated procedures (Attorney General Guidelines) under that Executive Order, but mainly for the benefit of US persons.

Similarly, the December 2016 update to US federal rules of criminal procedure, notably Rule 41 on search and seizure, allows a magistrate judge (on request by a federal law enforcement officer, e.g. the US Federal Bureau of Investigation (FBI), or government attorney), with authority in any district where activities related to a crime "may" have occurred, to issue a warrant allowing remote access (including hacking) to search electronic storage media and to seize or copy electronically stored information located within *or outside* the judge's district, if the district where the media or information is located has been 'concealed through technological mean', or if, in an investigation of a violation of the US Computer Fraud & Abuse Act (unauthorized access to information in computers involving interstate or foreign communications), the media are protected computers (a very broad term) that have been damaged without authorization and are located in five or more districts. Obviously this rule could have very broad extra-territoriality, allowing the hacking of devices located outside the US where the location has been concealed.

Many may conceal their device's location for privacy reasons rather than nefarious purposes, for example organizations using VPNs (virtual private networks), and this rule will permit the hacking of innocent persons' computers that have been infected by botnets, for example, without limiting the scope of what can be searched or copied within those computers (see criticisms of rule 41 by civil society and technology organizations, including Google and PayPal).

So, ironically, efforts to keep personal data outside of the US may in fact make it easier for US authorities, at least as US law matter, to access that data.

4.7

p.148, final para. - interestingly, a different approach, and what I consider is the correct approach, is taken in the UK government's cloud security principles. Its principle 2, on asset protection and resilience, rightly states, in relation to the aspect of physical location and legal jurisdiction, that the need to identify locations relates to not just storage/processing locations but locations from which data are managed from (i.e. controlled). It further states that the reason is to understand the legal circumstances in which organizations' data could be accessed without their consent: in other words, the true issues are of legal compliance and legal jurisdiction, including jurisdictions 'within which the service provider operates', i.e. jurisdictions to which the provider is subject.

4.8

p.149, n.35 – as a recent example of the conflation of location with jurisdiction, and the fear that data crossing borders necessarily entails loss of control, a former Australian spy chief was reported as

saying that once data left Australia 'it was no longer protected by Australian sovereign law', although he then linked control of data with the ability to implement suitable arrangement and controls with external suppliers (which is not a data location issue!) and remarked that data 'sent offshore' should be encrypted so only the 'owner' could read it.

5. Chapter 5 – Mechanisms and derogations

5.1

p.152, first para. – guidance from the WP29 (which will become the EDPB) on transfers under the GDPR is expected during 2017 through updates of its existing 'opinions and referentials', according to WP29's 2017 action plan.

5.2.2.2

p.156, first para. – the list of countries so far found adequate by the Commission is available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

5.2.4

p.160, first full para. – in January 2017 the Commission published its strategic framework for adequacy decisions and other Mechanisms, setting out politically-pragmatic criteria for deciding with which third countries it should pursue 'a dialogue on adequacy' are: (i) the extent of the EU's (actual or potential) commercial relations with a particular third country, including the existence of a free trade agreement or ongoing negotiations; (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties; (iii) the pioneering role that country plays in privacy and data protection that could serve as a model for other countries in its region; and (iv) the overall political relationship with that country, particularly with respect to the promotion of common values and shared objectives at international level (Communication on 'Exchanging and Protecting Personal Data in a Globalised World', COM(2017)7 final, p.8-9). On that basis, the Commission will 'actively engage with key trading partners in East and South-East Asia, starting from Japan and Korea in 2017', also mentioning the possibility of India, Latin America particularly Mercosur, and the 'European neighbourhood' – which hopefully includes the UK post-Brexit, should the UK government decide to seek whitelisting for the UK; the tech sector has argued in the UK Parliament this would be the best solution for UK organisations, fearing restriction of data flows post-Brexit. Commissioner Jourová has stated it would be 'ideal' if the work for Japan and South Korea could be finalised in 2017. In March 2017, the Commission launched a dialogue on data protection and data flows with Japan (more details).

The Commission also indicated that it would consider partial or sector-specific adequacy, e.g. for the financial services or IT sectors or other economically-important industries or geographic areas in the third country, in light of the nature and state of development of the privacy regime (stand-alone law, multiple or sectoral laws etc.), the constitutional structure of the third country or whether certain sectors of the economy are 'particularly exposed to data flows' from the EU. It invited third countries for whom existing adequacy decisions were in place to inform it of any relevant changes in law relevant to their decision to ensure continuity of their decisions under the GDPR (COM(2017)7 final, p.9).

p.160, last full para. – in assessing the adequacy of a third country under the GDPR, the new explicit (but currently implicit) factor relating to public authorities' access to data (Art.45(2)(a)) is likely to be very relevant to future adequacy decisions. If a country is an EU Member State, part of the EU 'club', processing of personal data for national security purposes is exempt from the GDPR. However, a country that is not in the club, such as the UK post-Brexit, will find its authorities' access to personal data closely scrutinized, as occurred with the US during the Shield negotiations (and since). Given broad powers for authorities to access data under the UK Investigatory Powers Act 2016, some technology companies are reportedly even considering moving their datacentres out of the UK, or have already done so.

5.3.1

p.162, first para. of 5.3.1 – Secretary Penny Pritzker, in her Cabinet Exit Memo in January 2017, noted that the Privacy Shield framework was essential to support over $260 *billion* in cross-Atlantic digital services trade annually.

5.3.3.1

p.168 first para. – the WP29 issued EU-US Privacy Shield – FAQ for European Individuals (*WP246*) and EU-US Privacy Shield – FAQ for European Businesses (*WP245*) in December 2016.

The WP29 also adopted, in February 2017, a standard complaints form for complaining to national DPAs about US organizations under the Shield, and rules of procedure for submitting requests to the Ombudsperson via the 'EU centralised body' (which will comprise five national DPAs) under Shield Decision Rec.119 and Annex III as well as, in April 2017, a form for submitting requests to the Ombudsperson. It seems that no complaints have been made regarding the Shield, as at 21 March 2017.

The WP29 further adopted rules of procedure for an informal panel of DPAs under Shield Decision Rec.49ff. and Shield Principle III.5, to provide binding advice to US organizations following unresolved complaints from individuals about the handling of their personal data transferred under the Shield upon referral of the organization or the individual concerned, based on 'a pragmatic system of lead DPA handling the complaint and co-reviewers assisting the lead in its instruction work'.

5.3.3.3

p.168, last sentence – the Commission announced in March 2017 that the US Department of Commerce and the Commission had agreed that the first annual joint review of the Shield would take place in *September 2017*. Under Art.4(4) of the Shield Decision, the Commission "should evaluate" its adequacy finding regarding the Shield "within one year from the date of the notification of this Decision to the Member States" and annually thereafter, and the Decision was notified on 12 July 2016, so perhaps September is the planned publication (rather than review) date. I have also anecdotally heard that November 2017 may be the relevant date. The WP29 continued to reflect on the content of the joint annual review and DPA participation and, as at April 2017, had commenced discussions with the Commission on the organization of the joint annual review.

p.169, first para.

Trump Presidency and executive order

With the change in the US presidency, EU Justice Commissioner Jourová said that the Commission would 'closely monitor' the Shield's implementation under the new US leadership. The EDPS is reportedly sceptical (following privacy issues other than the executive order) that the Trump administration is 'serious' about meeting US obligations under the Shield.

In January 2017, US President Trump's executive order Enhancing Public Safety in the Interior of the United States included a Sec.14 on the US Privacy Act 1974: 'Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.'

This order triggered concerns, including on the part of Commissioner Jourová, about the viability of the Shield and calls to suspend it, even privacy concerns on the part of US senators who wrote to the US Department of Homeland Security accordingly, and requests by US technology organizations for EU concerns to be assuaged. However, reportedly the Commission noted that the US Privacy Act had 'never offered data protection rights to Europeans' and that the EU-US umbrella agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism would continue in effect,

relying on the Judicial Redress Act (see 7.5.3, p.313, n.116 and the update to that in this document) to extend the benefit of the Privacy Act to Europeans and give them access to US courts, although the EU would keep monitoring the implementation of both instruments and other US developments impacting on Europeans' data protection rights. Similarly, a letter to the Commission by the US Deputy Assistant Attorney General (Department of Justice) was reported in February 2017 to state that Sec.14 of this order did not affect 'the privacy rights extended by the Judicial Redress Act to Europeans', or 'the commitments the United States has made under the DPPA (Umbrella Agreement) or the Privacy Shield'. Also, the US Mission to the EU reportedly stated that the order does not affect the Shield because its protections do not depend on the Privacy Act. The FTC's acting chair Maureen Ohlhausen has said that it would 'continue to enforce the Privacy Shield protections... nothing has changed', and recently she reaffirmed the FTC's support for the Shield and its commitment of resources to enforce it actively: ' it has to succeed', given the importance of EU-US digital trade.

Similarly, it has been argued that the order may not be not as broad as feared (for example, arguably it is limited only to immigration issues rather than commercial transatlantic data flows) and that it does not undermine the Shield because it does not affect the Judicial Redress Act, under which EU nationals can still have redress before the US courts, and that indeed neither the Judicial Redress Act nor the Privacy Act (which concern privacy rules applicable to US government agencies) seem very relevant to *private* sector transfers under the Shield. However, it has obvious political consequences and it has been pointed out that the underlying US Privacy Act itself only provides limited protections. Furthermore, the new US attorney-general appointed under President Trump could change or revoke the January 2017 designations (see update in this document to 7.5.3, p.313, n.116) of the EU and EU countries concerned.

In February 2017, the WP29 noted its intention to write to the US authorities pointing out concerns and seeking clarifications regarding the possible impact of this order on the Shield and the umbrella agreement; requesting assurances on how US authorities will handle personal data regarding complaints under the Shield; and providing answers to questions from US authorities on the centralized body's functioning (for more on the centralized body, see this update document, on 5.3.3.1, p.168 first para.).

Also in February 2017, several civil society organizations wrote to the Commission and WP29 expressing concerns for the Shield in light of not only this order, but also the US Privacy and Civil Liberties Oversight Board (PCLOB) not having redress powers and even lacking a quorum in recent months. Indeed, even US senators wrote to the US Department of Homeland Security in February 2017, asking how the order would impact on the Judicial Redress Act and Shield.

In March 2017, in advance of meeting with US officials, Commissioner Jourová was reported as warning that the EU would 'withdraw' from the Shield or suspend it if the Trump administration did not ensure the privacy of 'European data'. However, after Commissioner Jourová's meeting that month with the new US Commerce Secretary (who had previously stated there was a 'tension' between privacy and 'problems of localization and data and the implications that they have for the internet'), she was said to be 'more positive' about the survival of the Shield, following his assurances that he understood the Shield's importance, while Commissioner Ansip seemed similarly positive after meeting new US Commerce Secretary Wilbur Ross. A speech by Commissioner Jourová at the end of March mentioned areas the Commission would keep a close eye on in relation to the Shield: 'there would be no Privacy Shield without Presidential Policy Directive No 28 and the Ombudsperson', and ' proper day-to-day implementation and robust follow-up' were vital.

In April 2017, following the WP29 chair's visit to the US, a WP29 press release pointed out that, despite the FTC and Ombudsperson's expressions of support for the Shield and willingness to assist on the Shield's forthcoming annual review, some key functions of the Shield's architecture were yet to be implemented following the US election, regarding the Ombudsperson, FTC commissioners and PCLOB, and the organization of the annual review remained to be discussed in detail particularly access to documents. It urged US authorities to provide concrete evidence that the Shield system was in place and worked effectively to provide real protection.

Yahoo email scanning

In October 2016, news broke about Yahoo! supposedly having, in 2015 (before the Shield was in place), adapted and deployed malware-scanning software to monitor systematically in realtime *all* Yahoo! customers' emails as they arrived, for certain information (a set of characters or 'selector' search term) requested by US intelligence agencies – not just stored emails, or targeted scanning of specific accounts only. Both Google and Microsoft stated that they had never engaged in such 'secret scanning' of email traffic. More specifically, the search was said to be under a 'secret court order' from a FISA judge for messages containing a computer 'signature' associated with a state-sponsored terrorist organization's communications, and stored and made available to the FBI copies of all emails containing those digital signatures, although that collection had since ceased. The constitutionality of using FISA for mass (as opposed to targeted) surveillance has been queried and US lawmakers wrote a letter to seek information and a full briefing.

Yahoo! said that the report was 'misleading' and that the scanning 'described in the article' did not exist on its systems. This news led to calls for the Shield to be suspended in consequence, and a question in Parliament, including regarding whether the Commission was aware of those activities and whether it would reconsider its adequacy decision on the Shield. The Commission answered that it was unaware during negotiations on the Shield, and had contacted the US authorities for clarifications. Reportedly Commission Jourová was 'not satisfied' with the initial US answers, which were 'relatively late and relatively general'. The Irish DPA also sought information from Yahoo! on the allegations and consumer organizations have urged other DPAs to investigate Yahoo!

In April 2017, the WP29 adopted and sent a letter to the US Office of the Director of National Intelligence (ODNI) on Yahoo!, copied to the Shield's Ombudsperson, seeking additional information regarding the legal basis and justifications for any surveillance activities concerning individuals 'subject to EU law'. Further information is awaited.

Other

In April 2017, the European Parliament adopted a resolution P8_TA(2017)0131 on 'Adequacy of the protection afforded by the EU-US Privacy Shield (2016/3018(RSP))' criticising the Shield's adequacy on various grounds including state surveillance and data sharing. This reversed the overall consensus in its resolution of May 2016 that was broadly in favour of the Privacy Shield (see p.167, first bullet point).

5.3.3.4

p.169, final para. – it was reported in December 2016 that the German and Czech governments have asked to be joined in to Digital Rights Ireland's case before the CJEU. Arguments as to why the Shield should be invalidated have been submitted, by Digital Rights Ireland and by La Quadrature. Technology organizations are, unsurprisingly, said to be concerned about the legal challenges, which have caused much legal uncertainty. In January 2017 it was reported that several applications to be an intervening party had been made, including by the US government, France, UK, the Netherlands, Microsoft and the Business Software Alliance. The hearing dates are still unknown.

p.169, n.23 – in December 2016 the CJEU issued its judgment in *Tele2*, ECLI:EU:C:2016:970. It ruled that the ePrivacy Directive precluded national legislation which, for crimefighting purposes, provides for 'general and indiscriminate retention' of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. It set out how legislation for targeted retention of such data, for fighting serious crime, should be circumscribed in order to be proportionate and valid.

It further held that Directive also precluded national legislation on the protection and security of traffic and location data and, in particular, access of competent national authorities to retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and (paras.114, 122) where there is no requirement that the data concerned should be retained within the EU. It is disappointing that this judgment has followed the line taken in *Digital Rights* (4.5.1, p.136, n.13), that data must be retained in the EU in order for an EU authority to control compliance with the Directive's protection and security requirements. As this book explains (see

Chapters 4 and 7 in particular), the physical location of digital data should not be equated with control over that data, but this judgment clearly continues that pre-digital approach.

5.3.4.1

p.173, last para – underlining the Restriction's Frankenrule status, the WP29's EU-US Privacy Shield FAQ for European Business (*WP245*), adopted in December 2016, states (Q.3, p.3) that (emphasis added) ' The fact that the recipient in US is member of the EU-US privacy Shield will enable European businesses to comply with the national laws implementing article 25 of the EC Directive 95/46, *but all other requirements as set up by the national data protection law remain applicable*'.

p.174, first full paragraph – as at 1 May 2017, IBM and Twitter have been listed as certified under the Privacy Shield, but not Apple or Yahoo! (see the Privacy Shield list). Interestingly, Yahoo! stated in its December 2016 SEC Form 10-K filing that 'We are not currently relying on the Privacy Shield Framework', but relies on SCCs 'and other mechanisms', which are 'subject to uncertainty and legal challenges'.

5.4.1.2

p.188, bullet points – the Commission has suggested that SCCs could be adopted for specific industries, business models and/or operators, e.g. for the health sector, or outsourcing services provided in third countries for European companies (COM(2017)7 final, p.10). New forms of SCCs could be adopted or existing ones supplemented with additional safeguards 'which could range from technical to organizational to business-model related solutions'. This approach has potential, if such solutions are permitted *instead of* certain contractual terms in SCCs, rather than in addition to them.

5.4.2.1

p.191, first para. and n.65 – the Commission stated that it would work with stakeholders on GDPR transfer tools, which 'may' include completing the work already commenced on processor-processor SCCs. However, such draft SCCs have been noted to be uncommercial – see n.65 – and no consultation with stakeholders on those SCCs seems imminent.

5.4.2.7

p.198 – the Irish court's ruling, in Schrems's case against Facebook regarding the validity of SCCs for transfers to the US, was reserved following conclusion of the hearing in March 2017. Judgment is expected in June 2017. *Data Protection Commissioner v. Facebook*, 2016 4809 P.

5.4.2.9

p.202, first full para. – in similar vein, in February 2017 Google announced that EU DPAs had confirmed that Google's agreements for international transfers for G Suite and Google Cloud Platform (GCP) were in line with the Commission's SCCs and should therefore not be considered 'ad hoc' clauses. Interestingly, Google stated that the WP29's review process was conducted in accordance with the *WP226* cooperation procedure for common opinions on contractual clauses' compliance with Commission SCCs. Unlike with Microsoft, the WP29 did not publish its letter to Google. The G Suite SCCs are available at https://gsuite.google.com/terms/mcc_terms.html.

5.4.3.1

p.205, n.100 - *WP155* was updated to rev05 in February 2017, but with no changes relating to data location.

5.4.3.3

p.208, first full para.– in its proposed Regulation to update the CIDPR (2.2.6 and updates thereto) consistently with the GDPR, the Commission states, regarding appropriate safeguards for transfers to third countries (p.11 of the explanatory memorandum preceding the text of the proposed Regulation), that 'Binding corporate rules, codes of conduct and certification mechanisms could be used, in accordance with [the GDPR], by processors other than Union institutions and bodies'. Similarly with Rec.54 of the proposed Regulation and its Art.49 on appropriate safeguards. Art.49(2)(d) allows as appropriate safeguards, without requiring specific authorization from the EDPS, 'binding corporate rules, codes of conduct and certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of [the GDPR], where the processor is not a Union institution or body'.

All this suggests that an EU institution/body may transfer to a processor that has BCR-P or an approved code/certification, *without more*. Clarification of this issue in relation to BCRs under the GDPR would be very desirable. If, under the GDPR, controllers may transfer to cloud providers and other processors who have BCR-Ps without needing further specific authorisation, BCRs would be much more attractive to processors. Certainly, in practice, there seems no good reason why controllers should not be able to rely on their processors' BCRs (containing extensive commitments by the processor) in order to transfer directly to the processor, particularly if the processor's BCR has been drafted so as to allow such direct transfers from controllers and has been approved by DPAs on this basis.

Unlike in the 'appropriate safeguards' provisions of the GDPR, Art.49(2)(d) of that proposed Regulation does not require 'binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights'. Perhaps that wording was omitted because those are required under the GDPR provisions on codes and certifications in any event.

5.4.3.4

p.209, first full para. - see update to 5.4.3.3, p.208, above.

p.209, second full para. – also, the Commission has suggested that 'sectorial [sic] needs can also be accommodated through BCRs applying to groups of companies involved in a joint economic activity, for instance in the travel industry' (COM(2017)7 final, p.10). However, as discussed in 5.4.3.4, it seems unlikely that this approach could be feasible in cloud.

5.4.5

p.210, penultimate para. – the Commission has indicated that codes/certifications could be developed as transfer-specific mechanisms, or alternatively as part of more general tools to demonstrate compliance with all the provisions of the GDPR (i.e. codes/certifications with specific cf. general scope), and highlighted the possible competitive advantage of having a privacy seal or mark (COM(2017)7 final, p.10). It also suggested (ibid. p.11) that it 'can' define requirements and technical standards for the establishment and functioning of certification mechanisms, including for aspects relating to international transfers (as it is empowered to do under the GDPR), but did not indicate any timetable for any such actions on its part.

p.211 last full para. – the C-SIG's Cloud Code of Conduct was handed over to its newly-established General Assembly in February 2017. It seems WP29 approval for the amended code still has not yet been secured.

6. Chapter 6 – Compliance and enforcement

6.4.2

p.240, last full para. – under the GDPR, controllers need no longer pay notification/filing fees, which in many Member States like the UK had contributed to the funding of national DPAs. With the abolition of such fees, DPAs will face resource issues, and in March 2017 the WP29 wrote to EU Member State governments to raise their awareness of these issues and urge them to provide sufficient resources to their national DPAS.

6.4.3.3

p.251, first para. – in November 2016, noting the massive increase in cross-border transfers of personal data particularly in cloud, notably SaaS office applications many of which are offered by US organizations (and therefore were thought to usually involve transfers), ten German DPAs announced a coordinated written audit and review of the transfers of randomly-selected 500 companies, large and small and from different sectors, with the objective of raising their awareness of transfers. This included specifically asking them about their use of products and services from external suppliers, which, in the experience of those DPAs, might involve transfers – such as remote maintenance, support, ticketing, but also customer relationship management or application management. The companies were asked to specify the relevant services and products they used and, if transfers were made, to indicate the basis such as the Shield, SCCs or consent. As at April 2017, this review is still ongoing.

p.252, first full para.– reportedly Microsoft requested an extension until January 2017. In January 2017 it announced various changes to Windows 10 which CNIL initially indicated seemed to comply, with the Swiss DPA stating that it was concluding its investigations as Microsoft had agreed to implement its recommendations (Switzerland, while not in the EU, has been found to be an "adequate" third country).

However, the WP29 wrote to Microsoft in February 2017 expressing continuing concerns regarding Windows 10, even with Microsoft's proposed changes. I would point out that those concerns related to Microsoft's legal basis for processing Windows 10 users' personal data, rather than transfers or the Shield, again demonstrating the emphasis on Principles rather than transfers per se.

6.4.5

p.256, last para. – the Commission has acknowledged that it is 'increasingly necessary' to enhance cooperation with relevant privacy enforcement and supervisory authorities of third countries, given multinationals' global reach, as global common action and interpretation/enforcement practices would benefit both individuals and organizations (COM(2017)7 final, p.12).

p.257, last para. and n.51 – illustrating the uncertainties regarding DPAs' powers, a concern was raised that Convention108 does not empower DPAs to share personal data under the Global Cross Border Enforcement Cooperation Arrangement, although the update to Convention108 (see 2.2.10 and the updates to it in this document) would to some extent, and it is countries' national laws implementing Convention108 that might conflict with this cooperation arrangement, but countries are not prevented by Convention108 from agreeing other complementary forms of cooperation (letter, expert's report). Further on this arrangement, FAQs are now available and information on how privacy enforcement authorities may participate.

p.258, last para. – the Commission indicated its intention to develop international cooperation mechanisms with key international partners to facilitate effective enforcement, including exploring the possibility of developing a framework agreement for cooperation between EU DPAs authorities and enforcement authorities in certain third countries, drawing on experiences in competition and consumer protection (COM(2017)7 final, p.13).

In the UK, the ICO is increasing its international engagement, such as through participating in the new Common Thread Network linking some 20 DPAs in Commonwealth countries.

7. Chapter 7 – Access and security

7.1.3

p.271, last para. – secure key management is notoriously difficult. In January 2017, Google launched its Google Cloud Key Management Service in certain countries, enabling customers to manage their encryption keys in a multi-tenant cloud service without an on-premise key management system or HSM (hardware security module). Customers can choose whether to store keys in-cloud or on-premise and can manage their own cloud-based keys or have Google Cloud Storage manage them. However, it is not clear what access Google would have to its customers' keys, which is of course important if authorities demand the keys from Google. In January 2017, Google also announced an initiative on key transparency, a directory to allow keys to be verified easily against their true owners.

7.2.

p.274, n.35 – in November 2016, Commission Vice-President Ansip echoed the view that cloud data 'will be protected like money in banks', whereas data in servers in basements may not be well protected.

7.2.3.1

p.277, third para. of 7.2.3.1 – in February 2017, Microsoft announced its preview of Storage Service Encryption (SSE) for Azure File Storage which, when enabled by the customer, automatically encrypts its data at rest stored with Microsoft, where Microsoft handles the encryption, decryption and key management. Further on cloud key management, see the update above to 7.1.3, p.271.

p.278, first para. – the March 2017 leaks of US Central Intelligence Agency's surveillance tools further demonstrate that encryption works, and is very difficult to break: if encryption not work, the Agency would not need to go to such lengths to intercept messages before they have been encrypted (or after they have been decrypted).

On email, work has progressed on the STS standard, April 2017 version available at https://datatracker.ietf.org/doc/draft-ietf-uta-mta-sts/. Organisations are also being urged to implement DMARC (Domain-based Message Authentication, Reporting & Conformance), an email authentication, policy, and reporting protocol, to help minimise fraudulent spoof emails that do not actually originated from the purported domain.

p.278, last para. – websites, for example the New York Times, have been increasingly enforcing SSL/TLS (HTTPS) encryption of browser transmissions, so that hopefully such adoption has reached tipping point and become the norm rather than the exception. For some ongoing statistics, see https://letsencrypt.org/stats/.

p.278, n.39 – in October 2016, Facebook completed rolling out end to end encryption for WhatsApp and Facebook Messenger.

p.279 – as an example, GoDaddy and Proofpoint have partnered to provide encryption of email in transit as an add-on service for users of GoDaddy's Office 365 services, even where recipients are outside the Office 365 user's organisation (such email is already encrypted at rest on Microsoft's servers).

7.2.3.2

p.283, first full para. - on providers not necessarily being 'processors', see update to 1.2.3, p.4-5.

7.2.3.3.2

p.285, n.60 – this source was updated in December 2016, see the References section of this update document. In 2016, an increased 62% of enterprises used the cloud for storing files in electronic form, 44% for database hosting, and 41% for office software (e.g. word processors, spreadsheets, etc.).

7.2.3.3.4

p.286, first full para. – as regards the breakability of encryption, I should mention quantum computing. Quantum computers will enable encryption to be broken much faster than hitherto. In computers, data is represented by patterns of bits, 0s and 1s (see 3.7.3, p.105 first para. and n.56). With quantum computers, bits could be 0 and 1 at the same time, so that quantum computers would be able to operate on data much faster than non-quantum computers can to try to 'crack' encryption. Work is progressing apace on producing practicable quantum computers, and quantum computing is considered a threat to security, with one September 2016 report estimating a one-in-seven chance that some of the main public-key cryptography tools currently used will be broken by 2026, and a 50 percent chance they will be broken by 2031.

However, that does not mean that encryption is futile: symmetric encryption using large keys is still thought effective. In the US, for organizations running national security systems, the NSA has issued guidance (difficult to find on US government sites but saved on Cryptome), with an associated Commercial National Security Algorithm Suite and Quantum Computing FAQ, recommending, effectively, using much larger key sizes, and moving to quantum resistant algorithms in the future (the NSA has started working on a new suite of algorithms), again with data security life (7.2.3.3.4, p.286) being relevant – see factsheet summarising the minimum recommended keysizes/parameters if using different current algorithms.

On cloud key management, see the update above to 7.1.3, p.271.

7.2.3.3.6

p.288 – the debate on encryption backdoors 'only' for authorities continues, and authorities seem to demand backdoors every time a terrorist attack occurs, such as the French and German interior ministers writing (in French – the following is based on online translations) to the Commission in February 2017, stating that the fight against terrorism required EU authorities to have 'legal means' to 'take account of' the widespread use of encryption in judicial and administrative investigations, and asking the Commission to ensure technical and legal work was conducted to explore the possibility of defining new obligations on the providers of electronic communication services 'while ensuring the reliability of highly secure systems' and to propose an appropriate legislative initiative in October 2017. While it is unclear, if this letter suggests backdoors (as many believe), the writers seem to have ignored the contradiction in terms, as implementing that would be at completely odds with 'highly secure systems'.

As another example, the UK Home Secretary called for backdoors in messaging app WhatsApp after the attack on Westminster Bridge near the UK Houses of Parliament in March 2017. The problem clearly persists of politicians not understanding how encryption works, or appreciating the dangers of insisting on backdoors, despite experts' warnings and many signing an open letter asking governments not to restrict encryption or require backdoors; the Internet Society in April 2017 reiterated to the G20 countries that encryption should be made stronger, not weaker, calling indeed for ubiquitous encryption for the Internet. All this highlights a much wider issue, that lawmakers' and regulators' inadequate understanding of technology generally have very serious adverse implications for privacy, security and innovation.

Echoing an earlier 2016 joint statement by EU security agency ENISA and EU law enforcement agency Europol, which took the view that 'Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well', in December 2016 ENISA published (news release) an opinion paper on encryption. Concurring with other technical security experts (some of whom cited in the book), and even some politicians,

ENISA stated that using backdoors in cryptography is 'not a solution. Existing legitimate users are put at risk by the very existence of backdoors. The wrong people are punished... Backdoors do not address the challenge of accessing of decrypting material because criminals can already develop and use their own cryptographic tools...'. It also took the view that law enforcement solutions need to be identified *without* using backdoors or key escrow (where keys are available to authorities – the risks were highlighted by world-class security experts many years ago); it is 'very difficult to restrict technical innovation using legislation', and, from history, legal controls 'are not always successful and may harm and inhibit innovation': US experience has shown that limiting the strength of encryption tools inhibited innovation and presented other countries with a competitive advantage. The (naive, misconceived and positively harmful) perception on the part of many lawmakers that backdoors and key escrow are possible could, in ENISA's view, even potentially undermine aspirations for a 'full embraced Digital Society in Europe'. Similarly, Apple's CEO has pointed out that 'a back door for good guys can also be a back door for bad guys'.

7.2.3.3.7

p.288, last full para. – other work is being conducted, particularly in cloud. A notable example is the development of keyless systems for secure distributed storage of data, based on secret sharing, the EU PRISMACLOUD project – particularly its Archistar. Data are encoded and split into several parts, each of which is unintelligible. Each part may be stored using a different cloud customer account, even distributed among different cloud providers, and/or on-premise. A minimum number of parts must be obtained and combined in order for the data to be readable in intelligible form. This scheme is designed to prevent someone who has access to only one part, or even several different parts, from accessing intelligible data, unless they have the required minimum number of parts. The focus is therefore not on encryption (thus avoiding complex key management issues), but more on access control: ensuring only authorised persons or applications can login to the relevant cloud accounts to access and combine the required minimum number of parts.

7.3

p.290, first full para. – in surveys of over 1000 technical professionals, Rightscale found that, as at January 2016, security had been supplanted, as what they considered to be the top challenge for cloud adoption, by lack of resources expertise while, in January 2017, lack of resources/expertise remained the top challenge and security concerns fell still further. More recently, some 53% of IT executives (albeit in the US rather than EU) considered cloud more secure than on-premise. According to an April 2017 study, perhaps reflecting the greater maturity of the cloud market in the US, half of IT decision-makers in the US actually viewed cloud as more secure than on-premise infrastructure, but the majority in Germany and the UK trusted their own datacentres the most. Tellingly, a representative of the UK National Cyber Security Centre stated in February 2017 that **'On balance we think well-engineered SaaS is better for security than the alternatives**' (see that link for detailed reasons why).

7.4.2.3

p.296, second full para. – Microsoft's Office 365 and Power BI Pro became available with the German data trustee option from January 2017; Azure was available from September 2016 and Dynamics 365 will be available 'in the first half' of 2017.

p.297, n.82 – Google's list of subprocessors is now at https://gsuite.google.com/terms/subprocessors.html and has been expanded to name all Google group affiliates which are subprocessors.

7.5.2.1

p.310, first full para. – in October 2016, Germany passed legislation allowing its intelligence agency Bundesnachrichtendienst (BND) to intercept the communications of foreign entities and individuals on

German soil and abroad passing through a major internet exchange point (IXP) located in Frankfurt, but the IXP operator, DE-CIX, has reportedly commenced litigation against the validity of that legislation.

7.5.3

p.313, n.116 – a list of countries designated as 'covered countries' under the Judicial Redress Act was published in the US Federal Register in January 2017 – not including the UK, to date. This is because, by Art.27 of the umbrella agreement further to which that Act was passed (see this document's updates to 5.3.3.3, p.169, first para.), Denmark, Ireland and the UK are excluded from coverage unless and until the Commission notifies the US that the relevant country has decided that the umbrella agreement applies to it. As at 1 May 2017, of those three countries only Ireland has so agreed and been notified (and it was accordingly designated in January 2017).

8. Chapter 8 – Summary and recommendations

8.8

p.331, first full para. – there have been many studies about the economic benefits of digital globalization, particularly for SMEs (and economic costs of data localization), e.g. by consultants McKinsey, and see the Economist's article about the economic and political/human rights dangers of "splinternet".

p.333, fourth full bullet point – block mechanisms - under the CIDPR (2.2.6 and update thereto in this document), it was noted that small institutions lack resources and skills to assess adequacy, hence it was recommended (evaluation study of CIDPR p.62, 122, 142, and associated analysis p.17) that they should be allowed to use model clauses validated by the EDPS as a 'block' mechanism, specifically citing the example of using a cloud provider, instead of institutions having to assess adequacy themselves as hitherto required by the EDPS. A draft Regulation proposed in January 2017 to replace the CIDPR effectively mirrors the GDPR in the transfers context, with some adaptations – see the update in this document to 2.2.6, p.36, first and second full paras. This includes (in the draft Regulation's Art.49(2)(b)-(c)) allowing EU bodies/institutions to use model clauses adopted by the Commission, or by the EDPS if approved by the Commission, under what would effectively be the same as the Art.93(2) GDPR committee mechanism.

9. References

CoE – the website has been changed since the main body of the book was finalized in October 2016, and most of the links given no longer work. Please use the following links:
CoE, 1989; CoE, 2000a; (the CoE, 2000b link still works); CoE, 2010; CoE, 2012; CoE, 2015; CoE, 2016a; CoE, 2016b and CoE, 2016c.

Commission 2007, 2013b, 2013c and 2014b – these documents are unpublished but copies may be downloaded from http://www.e-elgar.com/data-localization-laws-and-policy-companion-site.

Giannakouris, K. and Smihily, M., 2014. Cloud computing: statistics on the use by enterprises. *Eurostat*. Updated in December 2016. Available at the same link, i.e. http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

Hon, W.K., 2016c. – this is freely available online.

Hon, W.K., 2016d. – this is freely available online.

Microsoft, 2014. These terms are continually updated by Microsoft, and more recent versions are available at http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31