GSR-16 Discussion Paper

MAINTAINING TRUST IN A DIGITAL CONNECTED SOCIETY

Work in progress, for discussion purposes
Comments are welcome!
Please send your comments on this paper at: gsr@itu.int by 30 May 2016

This paper was prepared by Douwe Korff, Emeritus Professor of International Law, London Metropolitan University, Associate, Oxford Martin School, University of Oxford

CONTENTS

Executive Summary

1. The development of the global digital connected society requires trust and security, based on sound regulation of the use of personal data. However, this is hampered by conceptual differences between states as concerns privacy in a narrow sense and data protection in a broad sense, and by different views on the application of the basic norms to non-nationals and to people outside a state's territory (the issue of universality of human rights).

2. The answer can only be found in global acceptance of a broad human rights-based concept of data protection that states must apply to "everyone" affected by their actions, irrespective of nationality or legal status or the place where they live. The global digital connected society can only develop in and between states that accept this fundamental principle.

3. There is the beginning of global convergence in terms of the contents of and approaches in data protection laws, with a trend towards adoption of laws on the "European" lines, and the establishment of special, independent and adequately resourced privacy- or data commissioners with strong investigative and enforcement powers, as demonstrated by the "Model Laws" drafted with support of the ITU and the EU for the Caribbean, Central and Sub-Saharan Africa.

4. There is strong global support for closer and more effective cross-border cooperation, not least as concerns the development of rules and tools to allow international data transfers – *either* because they occur between countries that have effectively the same levels of protection, *or* because "appropriate safeguards" are provided by various means and mechanisms such as data transfer contracts, Binding Corporate Rules, sectoral Codes of Conduct, or privacy seals.

5. The "modernised" Council of Europe Data Protection Convention, which is open to all states (not just to European ones) can become a global reference for data protection on which mutual assistance and mutual recognitions can be built if (as intended) the revised Convention, like the "Model Laws", will be aligned with the new EU data protection rules. The Convention and the Model Laws can in this way between them become a bridge between the EU, the Council of Europe Member States, and the rest of the world in terms of free data flows.

However, there are also obstacles:

6. First of all, there are jurisdictional challenges in relation to:

- the duty of states to ensure data protection to anyone "within their jurisdiction" (see points 1 and 2, above);
- the application of national data protection laws extraterritorially to activities by people or companies – or even public bodies – in other states; and
- the increasingly common cross-border "pulling" of personal data by one state's agencies from servers or devices that are physically in another state.

7. The absence of agreed global cybersecurity frameworks hampers the development of a global privacy- and data protection framework.

8. The adoption of international trade agreements could also undermine the developing, global privacy- and data protection framework, unless it is made clear that restrictions on transborder data flows imposed to protect personal data shall not be regarded as “non-tariff barriers” to trade.

Recommendations

1. Where Telecommunication Regulators are involved in the enforcement of data protection laws (or elements of data protection laws), they should be independent and endowed with adequate powers, on the lines indicated in the “Model Laws”.

2. National policy makers should strive to revise and improve mutual legal assistance systems in relation to the obtaining of communications data from other countries for law enforcement purposes. The revised systems should fully respect privacy and data protection and include appropriate judicial safeguards.

3. Where cybersecurity laws or measures cover or touch on data protection (e.g., in relation to encryption or law enforcement of interference with communications or communication devices), they should respect the global data protection requirements.

Implementation of these recommendations will help to bring about the trust and security that consumers need, and that is the necessary foundation for the development of a global digital society.

Part 1: The broad context: Data, trust and security in the digital world

1.1 Introduction

Compared to a few decades ago, the overall environment within which governments, businesses and individuals operate and interact has changed fundamentally in technical terms. Computer processing power has continued to follow Moore's Law, with transistor density doubling every 18-24 months – around one thousand-fold in the last two decades. Computer storage capacity and communications bandwidth have both been increasing even more quickly, doubling every 12 months and hence a thousand-fold each decade.

These exponential increases have radically increased the ability of organisations to collect, store and process personal data. It is no surprise, therefore, that our world is increasingly saturated with sensors such as CCTV cameras and mobile phones, with biometric and electronic identifiers used to link data to individuals. In the digital world almost every communication, online activities such as payment, search and Web page access leaves behind detailed footprints.[1]

Companies have long used data mining and -analysis to improve their products and services – and their margins. In a world of "Big Data" and the massive generation of both non-personal statistical- and personally identifiable data in the "Internet of Things" (IoT)[2] enables evermore detailed (and evermore intrusive) mining and "profiling". Governments are increasingly adopting similar technologies, in analysing and exchanging information on individuals in response to fears over terrorist attacks – or even over obesity in children.

The activities of both companies and governments in these respects has also become increasingly transnational: the digital environment by its very nature is global; and the economic opportunities and societal risks both also increasingly require transnational cooperation – between companies (the new environment is built on increasingly complex chains of actors); between governments; and between companies and governments. These developments pose serious challenges in terms of consumer protection[3] and, indeed, to the maintaining of the Rule of Law in this environment generally.[4]

A 2016 ITU Report already noted the major monetary and economic impacts of the IoT, running to trillions of dollars annually within a decade; the societal impacts in particular in terms of "smart cities" with "smartly" controlled infrastructure, transport and buildings using "smart" meters, etc.; the impacts on individuals in terms of health- and care management (through IoT-enabled health devices). But it also stressed the major challenges in terms of costs and reliability, connectivity, user interfaces and addressing, and the regulatory implications of licensing and spectrum management, standards (including on interoperability), competition and customer lock-in, security and privacy.[5]

The paper seeks to provide a basis for discussion on how to maintain trust in a connected digital society. It does not seek to provide answers to the numerous questions and challenges relating to the global smart society, but it will explore major areas that deserve attention, with some very tentative suggestions about how progress could be achieved at the global regulatory level.

More in particular, the paper will discuss the special rules that apply to the processing of the personal data which lies at the core of the digital connected society. It looks at privacy and data protection rules (and at the differences between these concepts); at three core areas affecting trust and security in the digital environment: national security, public security and

cybersecurity, and international trade agreements in globalized seamless world; and at the roles and responsibilities of regulators in all these fields, and the relationships between them.

These are extremely complex issues, which the paper does not seek to resolve but rather to stimulate the discussion in an informed manner.

1.2 Consumer trust and technical security

The challenges posed by the new global digital environment will not be met, and the promised benefits of the IoT will not be reaped, unless two fundamental and related conditions will be fulfilled, globally: trust and security.

Consumer trust – or the lack of it – in the new digital environment has been identified in Europe as one of the main obstacles to the development of the Single Digital Market in the European Union[6] – and the same is undoubtedly true in relation to the even wider global digital commercial environment. However, a 2014 survey conducted by Accenture found that globally, only 45 percent of consumers have confidence in the security of their personal data and that there are variations in the level of trust with developed markets expressing less digital trust overall. Consumers in emerging markets, in particular in Latin America and Asia, are more trusting, with 50 percent having confidence in the security of personal data compared to 41 percent of consumers in developed markets[7].

These statistics are worrying as they suggest that as consumers are more exposed to the digital environment, their trust actually decreases.

Until consumers and citizens feel that they can trust the technologies of the new digital environment – that they are technically protected against online "identity theft", financial fraud, data breaches, privacy violations and other misuses and abuses of their personal data[8] – the administrative and economic benefits of the IoT and the wider digital environment will not fully materialise.

Trust thus, to a large extent, relies on security: security against technical failures and against deliberate attacks on the IT/IoT infrastructure – but also against undue interference with that infrastructure by official entities. If the technologies are unreliable – e.g., if "things" that are supposed to be interoperable in practice cannot "talk" to each other; or if systems go down and cannot be relied on – officials, businesses and citizens/consumers will rightly refuse to adopt them. If systems can be broken into by criminals and those criminals can help themselves to our money or our sensitive data, then we will not use those systems.

And if governments themselves undermine the security of the digital environment – e.g., by the installation of unsupervised "back doors" systems that could be subverted, or by breaking encryption codes or demanding the handing over of decryption keys in secret – then even upright citizens will shy away from the use of such systems unless they believe – trust – that such extraordinary powers are only used when manifestly justified, in a targeted rather than indiscriminate ("generalised") manner,[9] and with the strongest possible systems of authorisation and oversight. If the Rule of Law is either generally traduced in a country, or if (even in states that generally respect the Rule of Law) sections of the state – such as the security- and intelligence agencies – are felt to be above the Rule of Law and/or insufficiently open controlled, then again the citizen will not feel secure.[10]

1.3 Consumer trust and the regulatory framework

Consumer trust requires technical security and reliability. But it also requires a sound regulatory framework: sound regulations; good rules (including appropriately limited exceptions); and full and honest application and enforcement of those rules and regulations (and exceptions). However, Members of Consumers International, a global federation of consumer groups, have expressed serious concerns in this regard, with 80% feeling legislation and regulation relating to redress are ineffective at keeping pace with the digital economy, and 76% doubting the efficacy of enforcement.[11] In the remainder of this paper, we will look at some of the core issues relating to these concerns.

In the next part, Part 2, we will discuss the special rules and regulations that apply to the processing of the personal data which lies at the core of the digital connected society, i.e., at privacy and data protection rules (and at the differences between these concepts). In Part 3, we will look at a number of other core areas affecting trust and security in the digital environment: national security, public security and cybersecurity. And in Part 4, we will examine the roles and responsibilities of regulators in all these fields, and the relationships between them.

Part 2: Privacy, data protection, universality and free data flows

2.1 Global challenges; different concepts and approaches

The provision of digital services, Big Data and the IoT all centre on data, and increasingly on the linking of those data to the activities of individuals – be those consumers, employees or citizens (e.g., in self-quantification or staff- or consumption monitoring) or (possible) suspects (as in data mining and profiling by law enforcement- and national security agencies). The digital connected society runs on personally identifiable information (PII) or, as it is called in Europe, personal data. This often – and again increasingly – includes sensitive data, either directly, as in IoT-connected medical devices, or less obviously, e.g., through traffic- or location data that can reveal whether a specific person was at a specific place or meeting at a specific time, and with whom she interacted; or through Passenger Name Records (PNR) that can provide surprisingly revealing details of a person's health, religion or race (amongst other information).

In these regards, it should be noted that more and more data that might seem to be "non-personal" or that are said to have been "anonymised" can increasingly easily be (re-)linked to specific individuals. "Smart" electricity meters not only record statistics on usage over time – when analysed, the data can be surprisingly revealing about the occupiers of the house in question.[12] Data in supposedly "anonymous" "Big Data" datasets are unexpectedly, and worryingly, re-identifiable. Furthermore, if even truly non-personal datasets are used to create "profiles" (be that of typical consumers of a particular product, or typical patients, or typical criminals or terrorists), and those profiles are then applied to datasets to single out individuals that meet the profile – then that processing too can very seriously affect those individuals, who may be denied insurance, or a job, or access to a flight or even a country (or worse) on the basis of effectively unchallengeable algorithms.[13]

This raises fundamental questions about the rights of the individuals concerned. However, there are challenges even with the very phrasing of the issues, and of the rights concerned.

Specifically, as explained at 2.2., below, although they are closely related, there are conceptual differences between privacy and data protection that, in the global digital environment, cause tensions between states and hamper transnational regulation and enforcement and cross-border trade. These tensions and problems are further aggravated by historical differences in the protection of individual rights, in particular in relation to non-citizens and in the importance attached to the protection of personal data in different countries and regions (as discussed in section 2.3). In section 2.4, we will examine the extent to which the data protection instruments themselves offer possible solutions to these problems.

Two further complicating factors – different views on the depth of interference with privacy that can or should be permitted in the name of national security, public security and cybersecurity; and the possibility of international trade agreements overriding data protection – are discussed in Part 3.

2.2 Privacy and data protection

Historically, privacy was mainly concerned with the right of individuals "to be left alone" by other individuals or private entities such as newspapers.[14] This was also generally the way the right to privacy and the "right to respect for private … life" that are enshrined in the post-World War II UN International Covenant on Civil and Political Rights (1966) and other international human rights treaties were originally seen: as a limited, essentially "negative" right, imposing on the state (and to some extent, indirectly, on private entities) little more than a duty to refrain from interfering with the private sphere of individuals.[15]

From the 1970s, in the light of perceived threats of large-scale computerised (mainframe) databases, mainly in the hands of governments, some states began to develop wider concepts, aimed at countering this new threat – but less so on the basis of a perceived threat to privacy in the old sense (freedom from intrusion) than on the basis of a new view that it was wrong for individuals to be controlled by these new technologies. If privacy was about a right to be "left alone", the new right, data protection, was about power. It sought, and seeks, to protect individuals from those who hold information on them using that information to manipulate and control them. The fear was that the computer could be used to undermine human autonomy and personal freedom in broad senses and, if done on a wider scale, could undermine democracy and freedom itself. As it is put succinctly in one of the earliest (1978) national data protection laws in the world, France's *Law on Informatics, Files and Freedoms*:[16]

> Computer technology … may neither infringe human identity nor the rights of man, nor private life, nor private or public liberties.

Data protection in this wider sense – of a *sui generis* right to protection of "data subjects" against improper uses of their data by those owning those data ("data controllers") – is particularly strongly embedded in European law including the European Convention on Human Rights and the European Union's Charter of Fundamental Rights, as interpreted and applied by the European Courts (the European Court of Human Rights and the Court of Justice of the EU). However, as noted in the next section, it is increasingly adopted worldwide and reflected in many guidelines and model laws being discussed globally, and can therefore serve as a reference to develop a regulatory framework for the global digital connected society.

However, before discussing the global data protection instruments as such, it is important to note another major factor that impacts on the application and enforcement of privacy/data protection law in the global digital environment: the general historical move from citizens' rights to universal human rights.

2.3 Universality of human rights

It is one of the hallmarks of international human rights law since 1945, and one of its greatest achievements, that under modern human rights treaties and constitutions such rights must be accorded by states to "everyone", to all human beings within the "jurisdiction" of that state, "without distinction [or discrimination] of any kind",[17] including nationality or legal residence status – rather than just to citizens of a state, as often used to be the case, in particular under constitutions adopted in earlier centuries.[18]

Moreover, the concept of "jurisdiction" as used in the modern human rights treaties has been developed from a purely territorial one – under which the rights in question must be accorded to everyone on the territory of the state concerned (only) – to one that relates to the exercise of power. According to the modern view of human rights, as pronounced by the International

Court of Justice as well as by global and regional human rights courts and -fora, states must accord (almost) all the rights contained in the human rights treaties to which they are a party, to everyone over whom they in some way hold power, i.e., in respect of whom they *exercise* jurisdiction (including prescriptive and enforcement jurisdiction).[19]

More specifically, this means that when states or state agencies or -agents are active in the (by its nature transnational) digital environment, they are bound under international human rights law to respect those rights, also in relation to any effect their actions may have on people who are physically outside of the territory of the state concerned.[20] Indeed, under the doctrine of "horizontal effect" of human rights,[21] they are also required to ensure that private entities such as companies that are subject to their laws are also prevented from actions that would unduly interfere with the protected rights of the persons concerned – including foreigners physically outside the country in question.

Some states have not yet adopted this "universal" view of human rights in their domestic law – which is challenging in the digital environment, especially if such states take actions in the global digital environment (e.g., "tapping" into the global submarine cable communications network) that clearly affect the rights and interests of consumers and citizens elsewhere in the world.[22] As illustrated by the Snowden case, this has serious negative effects on the global regulatory system, as discussed in Part 4.

2.4 The regulation of global personal data flows in the main international data protection instruments and model laws

2.4.1 The dilemma

When (initially only European) countries began to adopt data protection laws in the late-1970s and -80s, these naturally imposed restrictions on the free flow of personal data to other countries, so as to avoid evasion of the rules. This posed a dilemma that persists to this day.

On the one hand, the free flow of data, including personal data, "contribute[s] to economic and social progress [and] trade expansion" and facilitates cooperation between public authorities in different countries as well as scientific and technical cooperation and improved telecommunication, which is all of benefit to both companies and individuals. On the other hand, for countries and regional bodies that accept that data protection is a fundamental right, the processing of personal data involved in this must respect that right "whatever the nationality or residence of [the persons concerned].[23]

If there are "a wide variety of national laws, regulations and administrative provisions" on the processing of personal data, establishing different levels of protection for such data (or if there are countries without any relevant law, providing no protection at all), this "may prevent the transmission of such data from the territory of one [country] to that of another [country]", and this difference can "constitute an obstacle to the pursuit of a number of economic activities" at the trans- and international level, "distort competition" and "impede authorities in the discharge of their responsibilities".[24]

A range of attempts have been made to resolve this dilemma. In the 1980s, first the OECD and then the UN adopted non-binding guidelines, with the recommendation that as long as countries "substantially" or "broadly" followed these guidelines in their laws or regulations (or even through self-regulation), other countries should not impede personal data flowing

to them. More recently, APEC has adopted a Privacy Framework that is also non-binding and relatively flexible in respect of transborder data flows.

The Council of Europe went further and already in 1981 adopted and opened up for signature a binding international convention on data protection, which is expressly open to non-Council of Europe states. This contains stricter, binding rules than the above-mentioned guidelines, also in respect of transborder data flows. It has been supplemented by an additional protocol and is also more generally being "modernised".

The most detailed and strictest rules were adopted by the European Union, in a range of data protection instruments that are now firmly linked to the right to data protection as enshrined in the EU Charter of Fundamental Rights, which (since the coming into force of the Lisbon Treaty) has binding – and indeed constitutional – status within the EU legal order. These instruments also impose strict rules on transfers of personal data to non-EU (and non-EEA) countries, if those countries do not offer "adequate" protection to the data. The Court of Justice of the EU has recently ruled that, because of the high status of data protection in the EU legal order, this "adequacy" requirement should be read as demanding that the other country in fact offers "essentially equivalent" protection to that required under the Charter. In addition, the EU rules contain important provisions extending the application of those rules to non-EU/EEA companies that offer goods or services to EU persons, or that "monitor the behaviour" of such persons, in particular online.

The European rules have been hugely influential globally. More than 100 countries have adopted data protection laws, many specifically drafted on the lines of the EU rules. This latter development has been facilitated in particular by the promotion by a number of regional organisations of "model laws" based on the EU rules and drafted with the assistance of the EU.

In this section, we will first, in the next sub-section, 2.4.2, describe the non-binding UN-, OECD- and APEC guidelines. In sub-section 2.4.3, we will look at the binding Council of Europe and EU instruments; and in sub-section 2.4.4, at the model laws. In sub-section 2.4.5, we will discuss the special problem of jurisdiction in the digital environment, as concerns data protection. In the final sub-section, 2.4.6, we will examine the prospects for a global framework.

We will focus on the rules on transborder data flows, while noting in more general terms the different levels of detail and strictness in the different rules (in particular, in the binding instruments compared to the non-binding recommendations), since these impact on the transborder data flows.

2.4.2 Non-binding guidelines

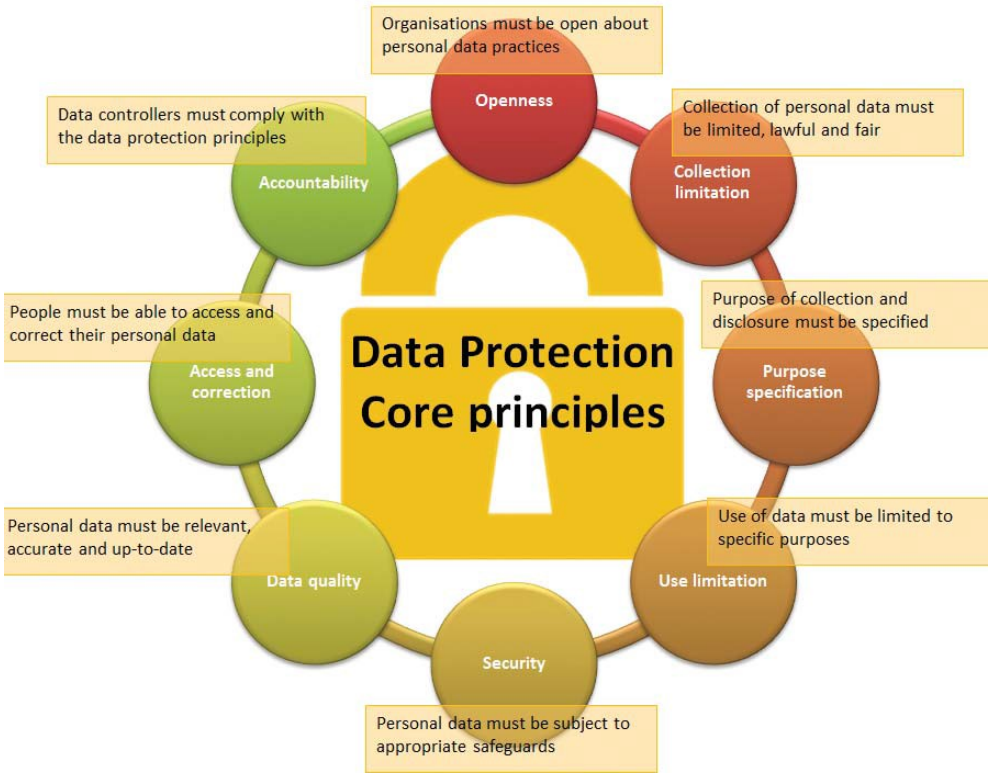
Non-binding guidelines have been adopted by the United Nations, the OECD and the Asia-Pacific Economic Community (APEC).

The first of these was the 1980 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.[25] These were revised in 2013 in the context of the creation of a wider OECD Privacy Framework that also includes new rules on privacy enforcement cooperation (that built on a 2007 recommendation on the issue).[26]

Some years later, in 1989, the UN adopted its own Guidelines for the Regulation of Computerized Personal Data Files.[27]

Most recently, in 2004, the Asia-Pacific Economic Community (APEC) published its Privacy Framework,[28] strengthened in 2007 by an APEC Cross-border Privacy Enforcement Arrangement (CPEA), further discussed in Part 4.[29]

With some variations, all of these share a set of common principles, which also lie at the basis of the binding instruments discussed at 2.1.2, below, as illustrated below:[30]



Source: UNCTAD /data protection regulations and international data flow: implications for trade and development http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

All three instruments seek to facilitate free data flows between states that have signed up to the relevant principles, as long as they broadly follow these – themselves already quite broadly-phrased – principles. As stated in the OECD Guidelines, "A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country **substantially observes** these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines (Para. 17, emphasis added)".

The UN and APEC guidelines follow similarly flexible broad principles: they all allow for quite different privacy and data protection systems – yet are aimed at mutual recognition of the adequacy of those different systems, as long they broadly meet the broad principles. Provided they follow these guidelines, the Member States of these organisations are encouraged to allow free data flows between them.

2.4.3 Binding regional data protection instruments with international reach

The first binding international instrument in the field of data protection was the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, better known as the Data Protection Convention (DPC) or "Convention No. 108" after its number in the European Treaties Series,[31] which in 2001 was augmented by an Additional Protocol regarding supervisory authorities and transborder data flows.[3233] As already mentioned, the Convention is in the process of being "modernised". The "Ad hoc Committee on Data Protection" (CAHDATA) appointed to this end has produced a Working Document with a Draft Protocol on the proposed amendments, which will to a large extent bring the Convention into line with the EU rules, noted next.[34]

In between the adoption of the Council of Europe Data Protection Convention in 1981 and the adoption of the Additional Protocol to that Convention in 2001, the European Union adopted, in 1995, the Data Protection Directive (or DPD for short).[35] A subsidiary directive on data protection in the field of electronic communications, known as the e-Privacy Directive, was further adopted in 2002.[36]

On 14 April 2016, the European Parliament approved, after a long legislative history, a new EU General Data Protection Regulation to replace the 1995 Data Protection Directive.[37] The new regulation is more detailed and strict than the 1995 directive and will be more uniformly interpreted and applied, through a number of new processes called the "cooperation-", "mutual assistance-" and "consistency mechanisms". It contains important provisions that are stricter in terms of extraterritorial effect and transfers of data to non-EU (and non-EEA) countries. Although the new regulation will not come into full effect until May 2018, it is already casting its shadow forward.

At almost the same time, on 11 April 2016, the Commission launched a consultation on its revision of the e-Privacy Directive, in which it will look at "possible changes to the existing legal framework to make sure it is up to date with the new challenges of the digital area."[38]

The EU has also adopted, or is in the process of adopting, a range of instruments on the processing of personal data by law enforcement agencies in the EU, and on the transfer and sharing of data for law enforcement purposes that have proved to be highly contentious, in particular in the light of a number of important judgments from the European Courts.

The requirements of the European instruments cannot be discussed here in detail. However, three aspects of direct relevance to the global digital connected world are described below.[39]

First, as noted at 2.2, above, data protection in a broad sense is regarded throughout Europe as a fundamental, universal human right.[40] In terms of EU law, it follows that personal data may only be transferred to another country if that other country provides protection that is "essentially equivalent" to the European standards, both in terms of substance and in terms of the availability of real and effective remedies.[41] Moreover, this protection must be provided by "the legal order" of the country in question;[42] and it must provide for effective remedies for "everyone" (i.e., not just for some categories of individuals, like nationals of specified countries).[43] The legal order of the other country must also protect against undue collection of data in bulk – and may in any case not provide for "generalised" – i.e., indiscriminate – access by the country's authorities to the content of communications.[44] These restrictive transfer requirements of EU data protection law are expressly allowed under the proposed revised text of the Council of Europe Data Protection Convention.[45]

However, the Regulation also envisages the provision of "suitable safeguards" by companies or groups of companies or sectoral bodies, in the form of data transfer contracts, Binding Corporate Rules or (typically sectoral) Codes of Conduct, subject to approval of such instruments by the data protection authorities (or at the European level, by the newly-established European Data Protection Board).[46] The EU Commission and (subject to EU-level approval) the national authorities can also issue "standard transfer contracts" (and have already done so under the 1995 Directive); and suitable safeguards for transfers can also be provided through privacy seals, through newly-regulated certification mechanisms. While there are still many questions about the operation of these mechanisms, they might provide the means to link the new European rules to the wider, global data protection regime (as noted in the next sub-section). The proposed revised text of the Council of Europe Data Protection Convention again expressly (albeit in broader terms) confirms this approach.[47]

Second, although they are built on the same "core principles" as the non-binding UN-, OECD and APEC guidelines, the European instruments are much more detailed and strict – the new EU General Data Protection Regulation alone runs to 149 pages of small print, with 99 long articles with numerous sub-clauses. They are, moreover, supplemented by very extensive, even more detailed recommendations and guidance from specialised bodies that generally further interpret the rules strictly.[48]

Third, it is an EU Charter requirement that the implementation of data protection law in the EU Member States be supervised by an independent authority. In several cases, the EU Court of Justice has underlined that data protection supervisory authorities have to remain free from any external influence, including the direct or indirect influence of the state; and indeed that the mere risk of political influence through state scrutiny is sufficient to hinder the independent performance of the supervisory authority's tasks.[49] The GDPR sets high standards for the relevant regulators in this regard;[50] specifies the tasks they must be authorised to perform, including handling complaints and carrying out investigations of their own motion;[51] and also requires that they be vested with very extensive powers of enforcement, including:[52]

- carrying out investigations and data protection audits;
- demanding access to premises and equipment used in processing;
- issuing warnings, reprimands and if needs be orders to data controllers;
- imposing "a temporary or definitive limitation including a ban on processing";
- ordering the suspension of data flows to recipient in non-EU countries; and
- imposing "administrative fines" for non-compliance with the Regulation or such orders, of up to 4% of annual turnover of the controller.

The Additional Protocol to the Council of Europe Data Protection Convention also requires the establishment of an independent data protection authority with broad powers and the proposed revised text of the Convention (if adopted as drafted) will bring this requirement into the main Convention framework.[53] As noted in sub-section 2.4.6, below, and in Part 4, this has implications for the nascent global data protection regime.

2.4.4 Model laws

Both the Council of Europe and the European Union have given extensive assistance to many non-European countries in the drafting of privacy- and data protection laws, drawing on the European instruments (the Council of Europe Data Protection Convention and the EU Data Protection Directive) discussed above.

Moreover, within a global ITU-EU-ACP project, the ITU and the EU (and others) have undertaken extensive work towards the establishment of harmonised policies for the ICT market in the African, Caribbean and Pacific (ACP) countries. This has resulted in the writing of a number of "Model Laws" and guides governing data protection (and others covering cybercrime and other matters). These include, specifically:

- HIPCAR: Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean:[54]

  Privacy and Data Protection: Model Policy Guidelines & Model Legislative Texts (2012)

- HIPSSA: Harmonization of ICT Policies in Sub-Saharan Africa:

  Southern African Development Community (SADC):[55]

  SADC Data Protection Model Law (2013)

- Model Laws Project of the Economic Community of Central African States (ECCAS) & Directive Project of the Economic and Monetary Union of Central Africa (CEMAC):[56]

  Model Law/Directive Relating to the Protection of Personal Data (2013)

  (contained within a broader publication on Cybersecurity Regulation)

All the above "model" instruments are clearly inspired, in terms of definitions, core principles, even structure and specific issues addressed, by the European data protection rules, in particular the 1995 EU Data Protection Directive.

Notably, they all also adopt the basic approach of the EU data protection instruments in relation to transfers of personal data to other countries: they stipulate that such transfers should in principle be prohibited unless the other country in question has adopted a law on the basis of the relevant Model Law, or otherwise ensures "comparable levels" of protection/an "adequate level" of protection, while also allowing for alternative means of providing safeguards, in particular through contract clauses.[57]

2.4.5 Jurisdiction

The question of jurisdiction is a major general problem in the inherently frontierless digital environment.[58] As the renowned Professor of Law Teresa Scassa and Robert J. Currie put it: "because the Internet is borderless, states are faced with the need to regulate conduct or subject matter in contexts where the territorial nexus is only partial and in some cases uncertain. This immediately represents a challenge to the Westphalian model of exclusive territorial state sovereignty under international law."[59]

In relation to data protection, the three main (linked) issues are:

i. The duty of states to ensure data protection to anyone "within their jurisdiction";

ii. The application of national data protection laws extraterritorially to activities by people or companies – or even public bodies – in other states; and

iii. The increasingly common cross-border "pulling" of personal data by one state's agencies from servers or devices that are physically in another state.

Briefly, the following may be noted in respect of these three issues:

Re i.: In sub-section 4.2.3, above, we have already shown that under modern human rights law, states have a duty to apply privacy- and data protection safeguards to "everyone within their jurisdiction", and that the latter term is now given a functional rather than a territorial meaning (even if some states do not apply it).

This widely-interpreted "jurisdictional" duty is clearly expressed in EU law (both in the Charter of Fundamental Rights and in the data protection rules). The EU guarantees data protection to "**everyone**" affected by any processing of their personal data by EU-based controllers, irrespective of where the affected persons (data subjects) are.

The Council of Europe Convention, in its original (still current) 1981 version is still restrictive in this regard; it stipulates that its purpose is to secure data protection rights for every individual "**in the territory of each Party**" (Article 1). These words have however been deliberately deleted from the proposed new "modernised" text of the same article. This must now be read together with the proposed new Article 3(1), which stipulates that:

> Each Party undertakes to apply this Convention to data processing **subject to its jurisdiction** in the public and private sectors, thereby securing every individual's right to protection of his or her personal data.

Specifically, in the wider Council of Europe area, too, the term "jurisdiction" must be read in functional rather than geographical terms, if only because the European Court of Human Rights has given the term such a wider application (see again sub-section 4.2.3, above).

The non-binding guidelines are by their nature less clear on this issue – but the OECD Guidelines reflect some of the same thinking where they stipulate that a data controller remains accountable for personal data under its control without regard to the location of the data (paragraph 16).

The Model Laws all also basically reflect the modern, broad view of the need to extend data protection to everyone affected by a state's action.

Re ii.: The non-binding UN-, OECD- and APEC guidelines are essentially silent on the question of whether, and if so when, states can extend the application of any laws adopted on their bases to actions by people, companies or public bodies in other states.

By contrast, the 1995 EU Data Protection Directive requires all EU Member States to apply their data protection laws to any company headquartered outside the EU if it sets up an establishment in an EU Member State, when this local establishment "orientates its activity towards the inhabitants of that Member State" (Article 4(1)(a) as interpreted in the *Google Spain* judgment of the CJEU, the so-called "Right To Be Forgotten" case).[60] The Directive also requires Member States to apply their law to any non-EU company (even without an establishment in their territory) which uses "equipment" or "means" in their territory to

process (e.g., collect) personal data on individuals in the EU (Article 4(1)(c)).[61] It is not entirely clear when this can be said to be the case, but the Article 29 Working Party has held that this can include the use of agents (physical or legal persons) as well as the use of cookies or Javascript banners (as long as this is not applied in cases with only tenuous links to the EU).[62]

The just-adopted General Data Protection Regulation clarifies and extends this further: Article 3(2) stipulates the following:

> This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

In relation to the Internet, "monitoring of the behaviour" of consumers in the EU can be said to take place in particular if the company uses "tracker cookies" or other online tracking tools.

The Model Laws, being generally inspired by the 1995 EC Data Protection Directive, tend to follow the approach of that directive. Thus, the HIPCAR Model Legislative Text on Privacy and Data Protection stipulates in Article 5 that:

> This Act applies to a the [*sic*] Data Controller in respect of any data if –
>
> a. the Data Controller is established (ordinarily resident, incorporated or branch office) in [Name of Member State] and the data is processed in the context of the business of that establishment; or
>
> b. the Data Controller is not established in [Name of Member State] but uses equipment in [Name of Member State] for processing data otherwise than for the purpose of transit through [Name of Member State].

This follows Article 4 of the Directive almost *verbatim*. Note in particular the reference in Article 5(a) to "branch office", which echoes the CJEU *Google Spain* approach. The reference to "equipment in Article 5(b) appears to be the result of the Model Legislative Text being based on the English language version of the EC Directive.

Re iii.: It is becoming increasingly common for state agencies – in particular law enforcement and national security agencies – to use the global digital infrastructure to "pull" data directly from servers or devices in other countries, without using the traditional processes under Mutual Legal Assistance Treaties (MLATs), or indeed without in any other way having obtained the consent of the targeted state. This is highly dubious in terms of general public international law, in that (outside times of war) such actions constitute the exercise of "enforcement jurisdiction" in another country, which violates the sovereignty of the other country.[63] Indeed, in cybercrime law, such unauthorised "equipment- or device interference" is now almost universally regarded as a criminal offence. Agents of the state making it a criminal offence may be granted special exemptions (e.g., in rules allowing law enforcement bodies to intercept communications subject to certain substantive and procedural requirements), but those do not normally extend to actions by foreign agencies. As explained elsewhere, Article 32 of the Council of Europe Cybercrime Convention (also known as the

Budapest Convention), which seems to permit such cross-border "pulling" of data, was never intended to be routinely used for such purposes.[64]

In this regard, there is something of a conflict between law and practice. On the one hand, as just noted, it would appear that such practices are contrary to international law. On the other hand, if anything those practices are spreading (or at least are becoming increasingly exposed in the wake of the Snowden revelations). Yet it cannot be argued that this widespread practice constitutes (the beginning of) new customary law, because there is no *opinion iuris*: although many states engage in the practices, there are few clear statements to the effect that they are accepted as lawful. On the contrary: most states at the receiving end of such practices protest strongly when such activities of foreign agencies are exposed. That is the opposite of accepting the practice as lawful.

In sum:

i. States are increasingly adopting national or regional data protection laws that extend data protection to everyone affected by a state's action, even if the affected persons are outside the physical territory of the state in question;

ii. States are increasingly adopting national or regional data protection laws that extend their application also to activities of foreign companies if those foreign companies either have an establishment in the country concerned or use "equipment" in the country in question to process (and in particular to collect) personal data on people in that country;

yet:

iii. States are also still allowing or at least condoning cross-border data-"pulling" activities by their law enforcement and national security agencies that appear to be *prima facie* in breach of public international law and that also unlawfully interfere with the privacy- and data protection laws and rights of the foreigners affected.

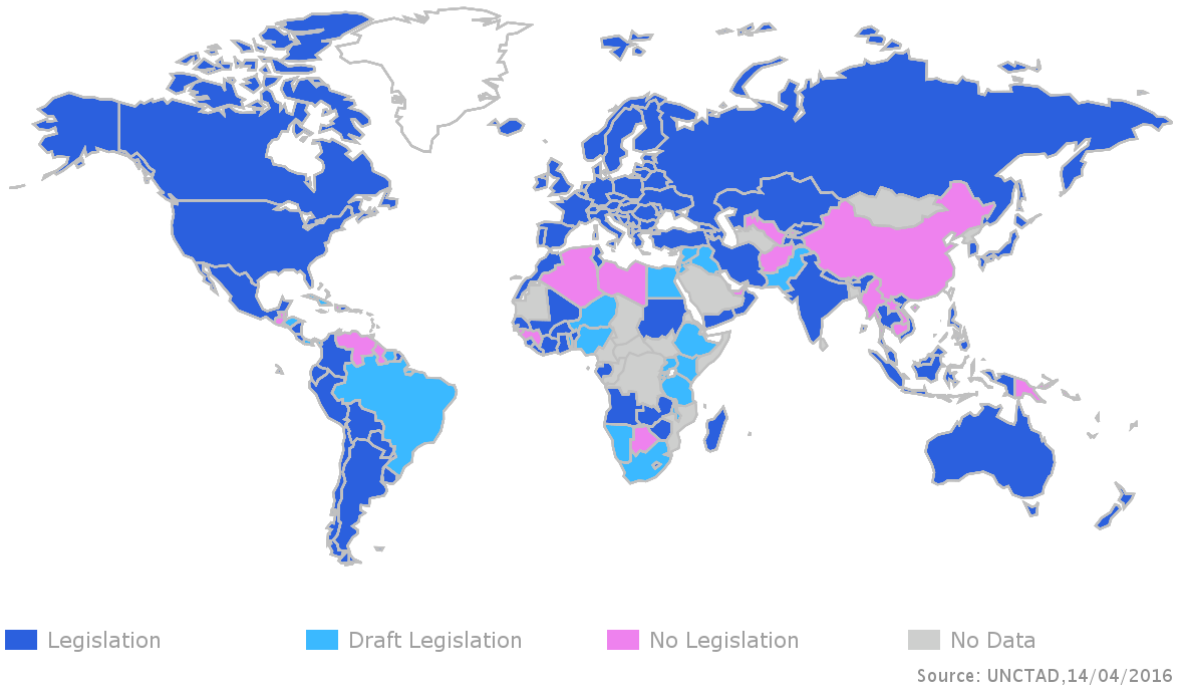
We will return to the latter issue in Part 4.

2.4.6 Data protection: global convergence and cooperation

The laws in many countries are clearly inspired by, and often closely modelled on, the European instruments, the 1995 EU Data Protection Directive in particular. Overall, more than 100 countries have adopted privacy- or data protection laws, as shown overleaf,[65] and it would appear that over time these are being strengthened in the direction of the "European" standards. A recent UNCTAD report[66] noted that governments "specifically in those developing countries attempting to adopt data protection legislation – are having problems modelling their data protection regimes, though most opt for an approach consistent with the EU Directive".

The Council of Europe Data Protection Convention – which has in any case been ratified by all the organisation's 47 Member States[67] – is open to all countries in the world and has in fact been acceded to by Uruguay; four African states are due to also become full parties to it: Mauritius, Morocco, Senegal and Tunisia. More are expected to join in the coming few years, in particular once its "modernisation" is concluded. Six non-EU states (Andorra, Argentina, Australia, Canada, Switzerland and Israel) have been formally declared to provide privacy rules that are "adequate" in terms of the EU rules.

Data Protection and Privacy Legislation Worldwide



This trend is reinforced by increasing support for stronger global privacy- and data protection laws given by the global intergovernmental- and human rights bodies. In the wake of the Snowden revelations, the UN General Assembly adopted a resolution on the issue in 2013,[68] which led to a report by the High Commissioner for Human Rights on the promotion and protection of the right to privacy in the digital age [69] and the appointment of the new UN Special Rapporteur on Privacy, Joseph Cannataci.[70]

The Revised OECD Privacy Framework and its guidelines have, over the years, been implemented increasingly strictly and in more detail. While the Revised OECD Privacy Guidelines still stipulate that Member countries should refrain from restricting transborder data flows to other countries that "substantially observe" the Guidelines, they also strongly encourage the adoption of appropriate safeguards. As the Supplementary Explanatory Memorandum to the 2013 Revised Guidelines put it, with reference to Article 17(b):[71]

> [This paragraph] gives recognition to the measures which a data controller can put in place to ensure a continuing level of protection, which may result from a combination of measures, such as technical and organisational security safeguards, contracts, complaint handling processes, audits, etc.
>
> However, the measures provided by the data controller need to be sufficient and supplemented by mechanisms that can ensure effective enforcement in the event these measures prove ineffective.
>
> Paragraph 17(b) therefore includes as a consideration the availability of effective enforcement mechanisms which support measures adopted by the data controller. Such enforcement mechanisms may take a variety of forms, including for example, administrative and judicial oversight, as well as crossborder co-operation among privacy enforcement authorities.

The reference to the need for "effective enforcement mechanisms" clearly relates to the fact that the existence of such mechanisms is seen as crucial in the EU rules and the Additional Protocol to the Council of Europe Convention (which will be brought within the main text of the Convention in the "modernisation" process).

From the EU's side, Article 50 GDPR expressly requires the EU Commission and the data protection authorities of the EU Member States to be active in this regard:

EU Data Protection Authorities must:

- develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
- provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and
- promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

There is therefore clearly at least the beginning of some convergence in terms of the contents of and approaches in data protection laws, with a trend towards adoption of laws on the "European" lines (cf. also the first two points in the summary at the end of the previous sub-section). And there is strong global support for closer and more effective cross-border cooperation. It may be hoped that once it is revised and "modernised", the Council of Europe Data Protection Convention, which as mentioned is open to all states (not just to European ones) can become a global reference for data protection on which mutual assistance and mutual recognitions can be built. In other words, a tentative global framework is slowly emerging. This will be further discussed in Part 4.

The next section, part 3, will examine the scope and range and cross-border application of special rules relating to national security, public security and cybersecurity (and indeed the lack of clarity with regards to these very concepts); and trade agreements, that all impact on privacy and data protection globally.

Part 3: National security, public security and cybersecurity, and trade agreements

There are two broad threats to the development of the global framework noted in Part 2:

- laws and measures in many countries that are aimed at the protection of national security, public security and cybersecurity often allow for very broad interferences with privacy and data protection, in widely varying ways and extents;

  and

- a series of proposed trade agreements which, their opponents argue, allow data protection laws (and other laws with socially beneficial aims such as protection of health and the environment) to be set aside if they threaten profits.

The challenges should be noted be noted before we discuss the future regulatory possibilities and difficulties.

Connectivity in a digital world also brings with it vulnerabilities at all levels and in all layers: in infrastructure and networks, transmission systems, hosting (clouds), apps and existing and innovative new systems and services (such as virtualisation and "softwarisation") and devices. Governments, businesses and individuals all seek protection against breakdowns, cyberattacks, fraud, data misuse, etc. – and as already noted, will not trust the digital environment until such protections are in place.

Protection in the digital world comes broadly in two forms: technical protection, and legal protection. These interrelate in that the law can stipulate or encourage the adoption of technical measures, set technical standards, and establish regulatory systems and -authorities. But the law can also allow for interferences with technical protection measures if these are believed to protect the wrong people: criminals, terrorists – and other, even less-defined targets. And it can either protect, or fail to protect, against abuses of technical measures that can have undue effects on the rights of individuals.

This poses serious dilemmas at national and international level, which have not yet been resolved.

Thus, on the one hand, security (e.g., against online and offline bank card fraud, or the physical security of an airport) can be enhanced by secure identification and authentication – which increasingly involves the use of advanced biometrics. But there are inherent dangers in the use of biometrics – including the uncontrolled matching of data from different sources, the surreptitious monitoring of individuals, and possible discrimination.[72]

There is also the question of whether individuals have a right to anonymity in the online environment. On the one hand, this allows people to access information on issues that may be contentious in their places of residence: e.g., political, religious, sexual or medical. Without protection of their identity, people in many countries would face serious consequences for even looking at such material. On the other hand, it allows "internet trolls" to post defamatory or threatening statements or material on the web, and religious and political extremists to disseminate hate speech and calls for violence, without risk of exposure for themselves.

Similarly, fully secure, unbreakable encryption allows citizens to feel confident in communicating and exchanging data and information with each other and supporting people and organisations worldwide; increases consumers' willingness to conduct more online

activities such as making payments, exchanging health records with their doctors, etc.; and enables whistleblowers to expose serious wrongdoings. But it also allows terrorists to plan their attacks in secret; and paedophiles to exchange images of child sex abuse. Yet breaking security and encryption risks breaking the whole security of the global digital environment: a vulnerability once detected and exploited by one actor (even a "good" one) can and will sooner or later be used by another ("bad") one.

All the international instruments discussed in Part 2 acknowledge the need for restrictions on the rights to privacy and data protection, where such restrictions are needed to protect general societal interests.[73] They also acknowledge that such restrictions should be based on law and be kept to the minimum necessary. However, the precise implications of these requirements are not at all clear – and the exceptions are clearly applied differently in different countries according to their regulatory regimes.

Furthermore, the very concepts – the aims for which restrictions may be imposed – are often not clearly defined, either in the privacy/data protection instruments, or indeed in national and international law generally.

Thus, in many countries the concept of "national security" includes the fight against organised crime and the protection of the economic interests of the state; is left deliberately undefined; at the discretion of the authorities; or can include the prevention of incitement to commit (apparently any) offences.[74] National security and "intelligence" agencies may be authorised to not just counter terrorism and other major threats such as organised crime, but also to gather information for political and economic purposes (even in the absence of any threat).[75]

"Public security" can similarly cover anything from serious and imminent threats to vague, non-criminal concerns; and "cybersecurity" is variously defined, by different organisations, to cover such diverse matters as:[76]

- purely technical security issues (protection against non-criminal threats to IT infrastructure);
- "cybercrime" (which itself covers very different things, from interception of communications and "hacking" to child pornography and hate speech);[77]
- the activities of law enforcement-, military- and intelligence agencies in cyberspace;
- some even add civil law and –procedure relating to e-contracts etc. –

The various sources also include in the concept of "cybercrime" anything relating to the above:

- in substantive law, procedure, oversight and remedies, national institutions, international instruments, and intergovernmental arrangements and –institutions;
- at the national and international/transnational level;
- and in national and international policy-making in these regards.

These conceptual issues are problematic because if there is no common, agreed understanding of the very concepts of "national security", "public security" and "cybersecurity", it will be impossible to arrange for good international regulatory cooperation on the measures taken to protect them.

In broad terms, individual-, human- and consumer rights are mostly obviously affected by measures taken by state and private entities to counter threats to national-, public- or cybersecurity in two main ways:

- if such measures involve monitoring of the activities of individuals in the digital online environment, the pulling of data on individuals (or that may also relate to individuals) from "cyberspace",[78] and/or the storing, sharing, analysing and further using of such data (e.g., for "profiling"); and
- if such measures are taken as part of criminal investigations (or may lead to such investigations).

These matters are complex enough in any single domestic context. However, the requirements become both more complex and more demanding if:

- the measures involve cooperation – and data exchanges – between state and private entities (companies, including in particular companies active in the digital environment, such as Internet Service Providers (ISPs), mobile network operators (MNOs) and social network service providers (SNSs);
- the measures involve cooperation – and data exchanges – between law enforcement agencies and national security agencies; and
- if there are transnational/international aspects to the measures, i.e., if they either involve actions of entities in one country that directly affect individuals (the data of individuals and the rights of individuals) in other countries (such as the pulling of data from a server in one country for analysis in another country), or if they involve cooperation between entities in different countries (which could be cooperation between private entities in different countries, or cooperation between public entities in different countries [such as international law enforcement- or national security cooperation], or cooperation between private entities in one country and public entities in another country).

It becomes increasingly challenging when these factors add up.

From the citizens' and consumers' perspective issues of serious concerns include:

- The indiscriminate "hoovering up" or otherwise accessing of massive sets of "bulk data" by intelligence agencies for use in data mining and profiling, in order to single out people who may possibly be involved in terrorism or other serious crime; and by companies to target prospective clients (or identify potentially bad customers). Decisions based on such data mining and profiling are subject to serious limitations and risks for consumers and citizens, including the risks of discrimination and high levels of "false positives" (because of the "base-rate fallacy"), but become effectively unchallengeable since they are based on increasingly complex, secret algorithms.[79]
- The installation of "back doors" into the servers and systems of electronic communication providers and others, through which state agencies have effectively uncontrolled full access to the data held and processed in and through those systems (i.e., without there being "data hand-over arrangements" as used to be in place in older systems), with "gagging orders" preventing the companies concerned from disclosing the existence of those doors, with severe penalties for any disclosure. They

also create vulnerabilities that can be exploited and thereby the security and reliability of the entire networks.[80]

- Demands for the weakening of encryption and/or the compulsorily making available of decryption keys by major Internet companies, including "cloud" providers, to allow "exceptional access" to data by state agencies. If the authorities that demand such weakening of encryption and handing over of keys are successful, this will undermine the security of the entire global Internet and electronic communications infrastructure, including the financial-, trading and even defence infrastructures: "encryption cannot be weakened 'just a little'".[81]
- The increasing trend of law enforcement and national security agencies "pulling" data directly from servers and devices in other countries in order to obtain evidence or intelligence – without using the traditional means for cross-border investigations, so-called Mutual Legal Assistance Treaties or MLATs.[82] This threatens to undermine both the established systems for mutual law enforcement assistance (although these do need urgent reform) and the emerging system of global data protection, discussed in Part 2, above.

International law, including international human rights law, on all these issues is still underdeveloped, but some of the basic principles and tests are beginning to be clarified in regional and international courts and other fora.

At the broader policy level, a number of organisations, including intergovernmental organisations, international defence-, trade- and financial organisations, academic institutions and major corporations are involved in a range of initiatives. This includes the ITU, which, with others, is in the process of producing a Cybersecurity Strategy Reference Guide and has already produced a Cybersecurity Strategy Toolkit;[83] the Global Cybersecurity Capacity Centre (GCCC) of the Oxford Martin School of the University of Oxford, which is working on a "Cybersecurity Maturity Model" (and which is also involved in the drafting of the Reference Guide);[84] and the Global Forum on Cyber Expertise (which includes both the ITU and the GCCC).[85]

However, this work is still very much in its infancy, with the focus for now being on the development of broad policies and strategies rather than on "details" such as how exactly the rules on national security, public security and cybersecurity should interrelate with the rules on privacy and data protection discussed in Part 2. In particular, apart from the, in this regard not yet very clear, limits imposed by human rights law, there are, at the moment, effectively no international frameworks regulating the work of intelligence services.[86]

Finally, we should mention proposed international trade agreements are currently being negotiated and which could impact on data protection. These include the proposed EU-USA Transatlantic Trade and Investment Partnership (TTIP),[87] the proposed EU-Canada Comprehensive Economic and Trade Agreement (CETA)[88], and the proposed Trans-Pacific Partnership (TPP) between the USA, Canada, Australia, New Zealand, Japan, Brunei, Malaysia, Singapore, Vietnam, Mexico, Chile and Peru.[89]

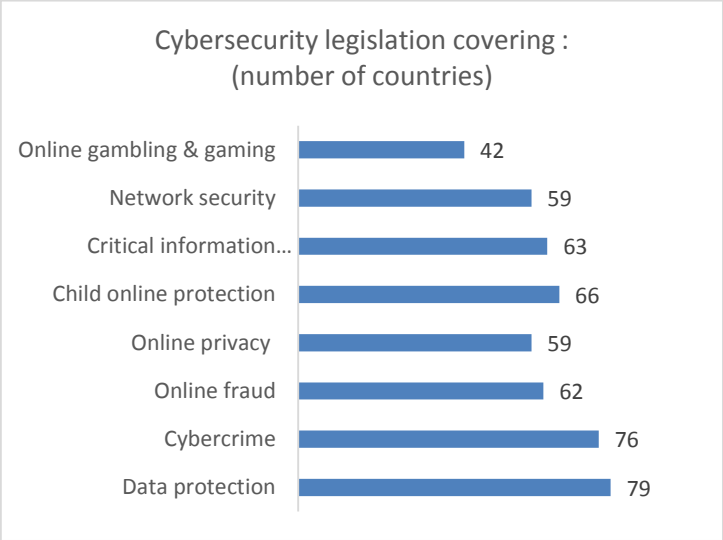
The debates generated by these proposed texts clearly highlight the importance citizens and consumers place in ensuring that these proposed trade agreements do not overrule data protection and privacy rights, in particular (but not only) in relation to transborder data flows and questions of jurisdiction.[90]

In sum: The absence of agreed global cybersecurity- and intelligence frameworks hampers the development of a global privacy- and data protection framework; and the adoption of international trade agreements could also undermine the latter, developing, framework, unless it is made clear that restrictions on transborder data flows imposed to protect personal data shall not be regarded as “non-tariff barriers” to trade.

Part 4: Roles and responsibilities of regulators

4.1 Different and overlapping frameworks

Today, different regulatory instruments and frameworks are regulating the digital ecosystem. Various entities may be in charge of overseeing data protection, privacy and security.



Source: ITU ICT Eye

According to ITU data, 73% of countries worldwide have adopted cybersecurity legislation (i.e., legislation covering all or most of the above kinds of broad issues). As the above chart shows, in 79 countries, data protection measures are included in such wider laws, while 59 countries have laws specifically dealing with online privacy. Cybersecurity (in this broad sense) falls within the mandate of the telecom/ICT regulator in more than 55% of the countries worldwide. This is the case of nearly 80% of the countries in Africa, 64% of the countries in Asia-Pacific and 61% in the Arab States.[91]

In many other countries both the regulatory frameworks and the regulators may be more dispersed. In Europe, as noted in Part 2, above, and further discussed below, at 4.1.2, special data protection laws and the establishment of a special data protection supervisory authority with strong enforcement powers are seen as essential, while in the United States, for example, there is no overarching privacy law but rather "a panoply of statutes" regulating different areas or practices, with different regulators with very different mandates and competences.[92] In a number of countries, the areas listed in the chart may be regulated in different laws (rather than all being brought under one overarching national cybersecurity law) and be subject to different regulators. In this report, we will continue to focus on the global data protection frameworks and the roles of data protection authorities (while also noting the need for them to cooperate with other regulators).

4.2 The emerging global data protection framework

As noted in a recent UNCTAD report, there is:[93]

> "a lack of clarity and compatibility between regimes add uncertainty, with negative effects on investments; and … given the nexus between cross-border e-commerce and data protection, divergent regimes will inhibit the adoption and proliferation of emerging technological developments, reducing potential accompanying societal benefits [but] Businesses are concerned that … too stringent protection regimes will unduly restrict activities, increase administrative burdens and stifle innovation."

To this should be added the crucial *caveat* that, not only in Europe but increasingly globally, important minimum requirements are increasingly firmly laid down in national constitutional and regional and global human rights- and consumer law: if those are deemed by other countries to be "too stringent" or "too high", it will be impossible to avoid risks such as compulsory data localisation that could lead to the fragmentation of the Internet and the global digital world. The same applies to the denial to provide for equal privacy- and data protection for "everyone" in some countries.

However, as noted in Part 3, challenges remain in relation to the largely unanswered question of what kinds and depths of interferences should be allowed to protect national security, public security and cybersecurity; and in relation to the tension between encouraging free cross-border data flows to enhance trade and restrictions on such flows to protect privacy.

It is difficult to agree on the basic rules, expanding on the agreed basic principles in relation to the many different contexts to be covered (ranging from employment to health to communications and much beyond). It will be much more difficult to agree on the application of the permissible exceptions for national security, public security and cybersecurity – and on providing protection against abuses of those exceptions to "everyone", including non-nationals. It is further likely that the issues relating to free trade and data protection will be equally difficult to resolve.

Still, at the international level, as noted in Part 2, there are signs of convergence in privacy- and data protection frameworks, and increased cooperation between relevant regulators, not least as concerns the development of rules and tools to allow international data transfers – *either* because they occur between countries that have effectively the same levels of protection, *or* because "appropriate safeguards" are provided by various means and mechanisms such as data transfer contracts, Binding Corporate Rules, sectoral Codes of Conduct, or privacy seals.

The OECD clearly encourages all relevant regulators in all OECD countries to cooperate with the EU authorities in this respect; and as we have seen, the Regulation in turn encourages the latter to reach out to regulators elsewhere.

However, again a similar *caveat* is required. The EU data protection authorities could be challenged if they were to agree to accept contracts, rules, codes or seals issued elsewhere, if those did not meet the constitutional (i.e., ECHR and EU Charter) requirements. Once again, therefore, the "Goldilocks Test" must in this particular context ensure compliance at least with the broad, fundamental global and human rights requirements. But provided that is done, they can be a major means of enabling a global data transfer regime pending the global adoption of statutory standards – provided, of course, that those standards are properly enforced.

4.3 Data protection regulators in practice

In Part 2 we noted that the Additional Protocol to the Data Protection Convention and, in particular, the EU GDPR set high standards for data protection authorities in terms of independence. The latter expressed this as follows:

EU General Data Protection Regulation

Article 52

Independence [of data protection supervisory authorities]

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

We also already noted in Part 2 that the GDPR requires that those independent DPAs be vested with extensive powers of enforcement [94] UNCTAD, adds that globally too:[95]

> Strong support exists for establishing a single central regulator when possible, with a combination of oversight and complaints management functions and powers. Moreover, the trend is towards broadening enforcement powers, as well as increasing the size and range of fines and sanctions in data protection.

This is reflected in the Model Laws. Thus, for instance, the HIPCAR Model Legislative Text stipulates that a Data Commissioner must be appointed, after consultation with both the Prime Minister and the Leader of the Opposition (S. 48); that that Commissioner must be independent in the exercise of his functions (S. 54) and may not be subjected to actions or proceedings in relation to acts done in good faith (S. 52); and that he must be vested with powers, *inter alia* to:

- control, inspect and verify processing operations;

- instruct data controllers "to take such measures as may be necessary to ensure that the processing of data is in accordance with [the data protection law]";
- investigate complaints from data subjects and from "associations representing data subjects" and take (impose) "remedial action as the Data Commissioner deems necessary or as may be prescribed under this Act, and to inform the data subjects or associations of the outcome"; and
- collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties

  (S. 55)

The EU data protection authorities have issued important, detailed guidance on the implementation of the EU rules, also in relation to the global digital environment, in particular through the so-called "Article 29 Working Party", already mentioned, in which they closely cooperate (this is shortly to be replaced, under the new General Data Protection Regulation, with a European Data Protection Board, but that board will still be composed of representatives of the EU DPAs, and the European Data Protection Supervisor).[96]

Again, such powers to issue guidance etc. are also envisaged in the Model Laws (cf. the HIPCAR Model Legislative Text, S. 55(f) and (j)).

However, it must be acknowledged that even in Europe DPAs have been less successful, and in some countries less willing, when it comes to actually enforcing the law and their interpretations of the law. This was made clear in a detailed comparative study of the authorities, commissioned by the EU's Fundamental Rights Agency, and published in 2010.[97] However, as noted in Part 2, the new EU General Data Protection Regulation grants the authorities stronger powers – including the power to issue fines of up to 4% of a company's annual turnover.

The FRA report also noted a "lack of data protection in the former third pillar of the EU" (police and judicial cooperation) – which is up to a point (but in the views of critics insufficiently) addressed in the recently adopted Law Enforcement Data Protection Regulation); and "a lack of clarity" regarding the extent of "broad exemptions and restrictions concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters), and the activities of the State in areas of criminal law" contained in the data protection directive. He added that:[98]

> In various Member States, these areas are altogether excluded from the protection of data protection law. This leaves a considerably large area unprotected with potentially serious consequences for fundamental rights protection.

That exclusion not only relates to the substance of the law (in the form of effectively or almost complete exemptions from the data protection requirements for the benefit of national security and other agencies); in many countries compliance with such data protection requirements as do apply is also not supervised by the normal DPA but by a special, usually less independent body, often with more limited powers than the normal DPA (e.g., in respect of access to the agencies' files).

Both globally and in the supposedly (in data protection terms) most developed areas (Europe in particular), state surveillance is still lacking in real and effective systems of control, authorisation and supervision.[99]

In other countries, supervision over compliance with data protection law may be split between different DPAs, e.g., different ones for the public and private sectors, or for different regions of the country. Although close coordination between such authorities in any one state is usually arranged for (e.g., in Germany, through the standing Conference of Data Protection Commissioners), such split authorities still add yet further complexity to an already complex area.

4.4 Other regulators

As noted earlier, the digital connected society may run on personal data, but the global digital environment is not only regulated by privacy and data protection laws – far from it. As the original explanatory memorandum to the OECD Guidelines already noted:[100]

> There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (e.g. with regard to the taking of evidence).

In fact, there can be many different authorities with responsibilities in different fields that may have a part to play in the regulation of the digital environment, that may complement, and can sometimes overlap with, the roles of DPAs. For instance, telecommunication regulators are generally responsible for supervising the activities of telecommunication network- and service providers – and they have in several countries been assigned supervisory functions in relation to, e.g., the use of traffic- and location data generated in mobile communications (regulated in the EU in the e-Privacy Directive), or compulsory communication data retention such as was mandated by the EU Data Retention Directive (since declared invalid – although several EU Member States still retain the relevant legislation).

In the Netherlands, consumer protection authorities are charged with enforcement of the regulations on cookies and other forms of online tracking of individuals (another matter regulated in the EU in the e-Privacy Directive).

In other countries, especially those with mainly sectoral data protection/privacy laws (such as the US), there are often a wide range of quite different privacy regulators, each with special competence in a special field (e.g., health, finance, travel), and often with differing powers and differing degrees of independence.

Such diffusion of responsibilities may not be conducive to effective regulatory supervision, in particular in the area of a constitutionally-protected right such as data protection. Such other agencies – well-intended though they may be – are usually not equipped or specialised to deal with human rights issues or relevant technical matters; and may lack the degree of independence of special data protection authorities.

To foster efficiency and effective protection of data, data protection issues should be under the supervision of specialised data protection authorities – but those should then be enabled (in terms of status, powers, financing and technical facilities) to take effective enforcement

action; and its heads and staff should be appointed in a way that ensures they are committed to taking such action where appropriate.

NOTES:

[1] Ian Brown, *Working Paper No. 1: The challenges to European data protection laws and principles*, (Introduction, p. 1), produced as part of a major study for the European Commission led by Ian Brown and Douwe Korff, New Challenges to Data Protection, 2010. The Working Paper is available at: http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_working_paper_1_en.pdf
The *Working Paper* goes on to provide extensive further detail of the developments briefly noted here, to which the reader is referred.

[2] The Internet of Things is defined by the ITU as:

> "*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication.*"

ITU-T Y.2060. For further discussion and references, see: http://www.itu.int/ITU-T/newslog/New+ITU+Standards+Define+The+Internet+Of+Things+And+Provide+The+Blueprints+For+Its+Development.aspx

The OECD puts it as follows:

> "*The Internet of Things consists of a series of components of equal importance – machine-to-machine communication, cloud computing, big data analysis, and sensors and actuators. Their combination, however, engenders machine learning, remote control, and eventually autonomous machines and systems, which will learn to adapt and optimise themselves.*"

OECD (2015), OECD Digital Economy Outlook 2015, OECD Publishing, Paris, available at: http://dx.doi.org/10.1787/9789264232440-en

[3] See: Consumers International, Connection and protection in the digital age: The Internet of Things and challenges for consumer protection, April 2016, available at: http://www.consumersinternational.org/media/1657273/connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf
See also the accompanying Briefing, at: http://www.consumersinternational.org/media/1657279/briefing-connection-and-protection-the-internet-of-things-and-challenges-for-consumer-protection.pdf

[4] Douwe Korff, The Rule of Law on the Internet and in the wider digital world, *Issue Paper* published by the Council of Europe Commissioner for Human Rights, 2014, *Executive Summary*, pp. 7 – 8, available at: https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CommDH/IssuePaper(2014)1&Language=lanAll&direct=true
(Choose language version)

[5] ITU, Trends in Telecommunication Reform 2016, chapter 5, Regulation and the Internet of Things, Ian Brown, 2016.

[6] See: Communication from the [EU] Commission to the Parliament, the Council etc., A Digital Single Market for Europe, *passim*, 6 May 2015 (COM(2015)192 final), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

[7] Accenture, The Four Keys to Digital Trust, 2014, available at: https://acnprod.accenture.com/t20150709T093453__w__/us-en/_acnmedia/Accenture/Conversion-Assets/LandingPage/Documents/3/Accenture-3-LT-7-Four-Keys-Digital-Trust.pdf

[8] On the differences between privacy in a narrow sense and data protection in the wider sense of protection against such misuses and abuses, see Part 2, section 2.2, below.

[9] On the difference between targeted and indiscriminate ("generalised") data access by state authorities, see Part 3, below, in particular the discussion of the case-law of the Court of Justice of the EU.

[10] See Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 4, above), Chapter 3: *The Rule of Law in the digital environment*.

[11] See: Consumers International, Connection and protection in the digital age: The Internet of Things and challenges for consumer protection (note 3, above), p. 40.

[12] See: EL Quinn, Privacy and the New Energy Infrastructure, SSRN Working Paper Series, 2009: http://ssrn.com/abstract=1370731

[13] See: Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, report for the Council of Europe Consultative Committee on data protection, June 2015, Council of Europe document T-PD(2015)11, section I.iii, *The dangers inherent in data mining and profiling*, available at:
https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

[14] See Samuel D. Warren and Louis D. Brandeis' famous essay, The Right to Privacy, Harvard Law Review, Volume IV, No. 5, December15, 1890, available at:
http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

[15] ICCPR, Article 17 (privacy); ECHR, Article 8 ("private and family life"). Note that in spite of the different terminology in English, the terms were at least originally envisaged as meaning the same thing, as is clear from the use in the authentic French versions of both instruments of the term "*vie privée*". Note that the international human rights treaties protect individuals first and foremost against intrusions by states; protection against measures by other individuals or private entities such as companies is only accorded through indirect, so-called "horizontal application" of these treaty rights. The international remedies accorded under these treaties, too, can only be used *vis-à-vis* states, who can however be held accountable for not protecting individuals from interferences by others.

[16] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, Article 1 (author's translation).
The German Constitutional Court expanded on this in its famous *Census* judgment in 1983 as follows:

> "*A social and legal order in which the citizen can no longer know who knows what when about him and in which situation, is incompatible with the right to informational self-determination. A person who wonders whether unusual behaviour is noted each time and thereafter always kept on record, used or disseminated, will try not to come to attention in this way. A person who assumes, for instance, that participation in a meeting or citizen initiative is officially recorded, and may create risks for him, may well decide not to use the relevant fundamental rights ([as guaranteed in] Articles 8 and 9 of the [German] Constitution). This would not only limit the possibilities for personal development of the individual, but also the common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizen.*"

Volkszählungsurteil, BVerfGE Bd. 65, S. 1 ff. (author's translation).

[17] The ICCPR uses the words "without distinction" (Article 2(1)), where the ECHR uses "without discrimination" (Article 14), but the effect is identical.

[18] The principle of universality of human rights was most clearly and simply, but emphatically, first expressed in the Universal Declaration of Human Rights, adopted by the U.N. General Assembly on 10 December 1948. The principle is also re-emphasised in the 1985 UN Declaration on the Human Rights of Individuals who are not Nationals of the Country in which They Live, although (as the title makes clear) this addresses the rights of people living in a state of which they are not a national rather than the rights of people affected by extraterritorially-applied laws and actions of states in which they do not live, but which affect them in the digital environment. For a more detailed discussion, see Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 2, above), Section 3.3, sub-section 3.3.1, *The principle of non-discrimination in international law*.

[19] *Idem*, section 3.4, *"Within [a contracting state's] [territory and] jurisdiction*", with extensive references to the relevant case-law.

[20] Such extraterritorial actions (or actions with effect in other countries) will also normally violate the sovereignty of the targeted state and thus be unlawful under public international law, see: Douwe Korff, Expert Opinion, prepared for the Committee of Inquiry of the German *Bundestag* into the "5EYES" global surveillance systems revealed by Edward Snowden, presented at the Committee Hearing, Berlin, 5 June 2014, available at:
http://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf (full text in English, in spite of what it says on the cover page):
http://www.bundestag.de/blob/282876/b90dd97242f605aa69a39d563f9532e7/mat_a_sv-4-3_korff_zusammenfassung-pdf-data.pdf (summary in English)
However, this is not further discussed in this paper.

[21] See note 15, above.

[22] See Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 4, above), Section 3.4, *"Within [a contracting state's] [territory and] jurisdiction*", under the heading "The US Government and the ICCPR".

[23] The quotes are from the second preamble to the 1995 EC Data Protection Directive, further discussed in sub-section 2.4.3.

[24] *Idem*, seventh preamble. The text there refers to data flows between EU Member States and obstacles to intra-EU trade etc., but the dilemma of course arises equally in other regions and trading zones, and at a wider, global level.

[25] OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980, available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[26] See: https://www.oecd.org/sti/ieconomy/privacy.htm
Chapter 4, *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011)* provides a very useful oversight of the historical developments on privacy generally.

[27] United Nations, Guidelines for the Regulation of Computerized Personal Data Files, UNGA Res. 44/132, 44 UN GAOR Supp. (No. 49) at 211, UN Doc. A/44/49 (1989), available at: https://www1.umn.edu/humanrts/instree/q2grcpd.htm

[28] Available at: http://publications.apec.org/publication-detail.php?pub_id=390

[29] Available at: http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf

[30] See the OECD Guidelines, Part Two ("Basic Principles of National Application"); UN Guidelines, Section A ("Principles concerning the Minimum Guarantees that should be provided in National Legislation"); APEC Privacy Framework, Part III ("APEC Information Privacy Principles").

[31] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in Strasbourg on 28 January 1981, CETS No. 108, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[32] Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, opened for signature in Strasbourg on 8 November 2001, CETS No. 181, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
The Additional Protocol was to a large extent aimed at bringing the Convention in line with the EU rules on the added matters (discussed later in the text), which were not or insufficiently addressed in the original Convention.

[33] Within the Council of Europe, data protection issues are further addressed by a number of bodies including the Parliamentary Assembly of the Council of Europe (PACE), a Consultative Committee, known as "T-PD", established by Convention No. 108, and the Council of Europe Committee of Ministers (COM or CM). Between them, they have issued many opinions, recommendations and studies in the area – always with reference to the Convention. See:
http://website-pace.net/en_GB/web/apce/documents (PACE documents) Note that these cover many more issues than just data protection – but they can be searched under the term "data protection". On 14 April 2016 this provided 265 results.
https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (T-PD documents);
https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (COM documents relating to data protection).
In addition, there is an interplay between the Data Protection Convention and the European Convention on Human Rights, with the European Court of Human Rights increasingly taking note of the Data Protection Convention and the above-mentioned kinds of documents in its own interpretation of Article 8 of the Human Rights Convention (which guarantees the right to private life); while PACE, the Consultative Committee and the Committee of Ministers in turn draw on the case-law of the Court in their work in this area. See the ECtHR Factsheet – personal data protection (note 16, above) and *Annex 1 – Jurisprudence* to a recent working document by the EU's "Article 29 Working Party", Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (note 41, below), which lists 15 important ECtHR judgments relevant to data protection (and five CJEU ones).

[34] Council of Europe Ad hoc Committee on Data Protection (CAHDATA), Working Document containing the Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), available at: https://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Draft%20amending%20protocole%20with%20reservations_En.pdf

[35] Full title: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, pp. 0031 – 0050, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[36] Full title: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002, pp. 0037 – 0047, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
In 2006, a further directive, known as the Data Retention Directive, was adopted, technically in the form of an amendment to the e-Privacy Directive, that required the compulsory retention of electronic communications data beyond the period for which those data would normally be retained by the relevant e-communications companies for their own business purposes, so that those data could be accessed and analysed by Member States' authorities "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law". Full title: Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, 13/04/2006, pp. 0054 – 0063, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
However, in 2014, in the *Digital Ireland* case (Joined Cases C-293/12 and C-594/12) the Court of Justice of the EU ruled that this directive was invalid because it did not meet the requirements of the European Union's Charter of Fundamental Rights (see Part 3, below). This Charter had become binding law within the Union by virtue of the Lisbon Treaty which entered into force in 2009. It guarantees both a general right to respect for private and family life, on the lines of the corresponding right in the ECHR (Article 7 CFR), but also the new, special *sui generis* right to data protection as developed in the EU Member States (as discussed at 2.1, above) (Article 8 CFR).

[37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal L 119, 04/05/2016, pp. 0001 – 00149, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

[38] See: https://ec.europa.eu/digital-single-market/en/news/public-consultation-evaluation-and-review-eprivacy-directive

[39] A fourth issue, the question of (extra-)territorial jurisdiction, is discussed separately in sub-section 2.4.5.

[40] For brief summaries of the ECtHR case-law, see the Court's Factsheet – personal data protection (note 16, above). The Article 29 Working Party has analysed the requirements that flow from the EU directives and the EU Charter of Fundamental Rights as interpreted in the case-law of the Court of Justice of the EU and of the European Court of Human Rights in a very recent, more extensive and thorough working document on surveillance, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), adopted on 13 April 2016, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf
Annex 1 – Jurisprudence to this document lists 15 important ECtHR judgments relevant to data protection: *Klass and others v. Germany*, 6 September 1978, Application no. 5029/71; *Malone v. United Kingdom*, 2 August 1984, Application no. 8691/79; *Leander v. Sweden*, 26 March 1987, Application no. 9248/81; *Huvig v. France*, 24 April 1990, Application no. 11105/84; *Hokkanen v. Finland*, 23 September 1994, Application no. 19823/92; *López Ostra v. Spain*, 9 December 1994, Application no. 16798/90; *Chahal v. United Kingdom*, 15 November 1996, Application no. 22414/93; *Amman v. Switzerland*, 16 February 2000, Application no. 27798/95; *Rotaru v. Romania*, 4 May 2000, Application no. 28341/95; *Copland v. United Kingdom*, 3 April 2007, Application no. 62617/00; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 28 June 2007, Application no. 62540/00; *Liberty and others v. United Kingdom*, 1 July 2008, Application no. 58243/00; *S. and Marper v. United Kingdom*, 4 December 2008, Applications nos. 30562/04 and 30566/04; *Gillan and Quinton v. United Kingdom*, 12 January 2010, Application no. 4158/05; *Bucur and Toma v. Romania*, 8 January 2013, Application no. 40238/02. All these can be found on the ECtHR's case-law (HUDOC) website: http://hudoc.echr.coe.int/eng

It also lists five CJEU judgments (including two already mentioned): *Commission v. Germany*, 9 March 2010, Case C-518/07; *Commission v. Austria*, 16 October 2012, Case C-614/10; *Commission v. Hungary*, 8 April 2014, Case C-288/12; *Digital Rights Ireland*, 8 April 2014, Joined Cases C-293/12 and C-594/12 (note 35, above); *Schrems v. Data Protection Commissioner of Ireland*, 6 October 2015, Case C-362/14 (note 41, above). All these can be found on the CJEU's case-law (CURIA) website:
http://curia.europa.eu/jcms/jcms/j_6/

[41] *Schrems v. Data Protection Commissioner of Ireland* (note 41, above), paras. 93 and 94. The Council of Europe Convention also refers to "equivalent protection" but in more ambiguous terms: see Article 12(3)(a)).

[42] *Idem*, para. 74.

[43] Cf. *idem*, para. 94; see also the Article 29 Working Party Working Document 01/2016 (note 47, above) and the Legal Opinion of the European Parliament's legal service (note 46, above).

[44] Such "generalised access" to communications content was held by the CJEU to infringe the very "essence" of the right to data protection: *Schrems v. Data Protection Commissioner of Ireland* (note 41, above), para. 73.

[45] Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (note 34, above), Article 14(previously Article 12), para. (1), added second sentence.

[46] GDPR, Article 46 (which must be read with the more detailed rules on the means mentioned and the stipulations on the powers of the authorities relating to these means and mechanisms).

[47] Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (note 34, above), Article 14(new)(3)(b), which stipulates that "[an appropriate level of protection can be secured by] … ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing."

[48] *Re* the Council of Europe, see note 33, above. For the EU, the 1995 Data Protection Directive established a body, somewhat prosaically referred to as "the Article 29 Working Party" after the article establishing it, which brings together representatives of all the data protection authorities in the EU and the EEA. It issues numerous opinions and working documents which, while not formally binding, are highly authoritative in terms of the interpretation and application of EU data protection law, and taken into account inter alia by the EU Court of Justice in its rulings on relevant matters. The Article 29 Working Party (WP29) opinions and working documents etc. can be found here:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
WP29 documents relevant to the global digital environment include (in reverse chronological order, from 2010 only): 2016: an opinion on the proposed EU-US Privacy Shield (WP238); a working document on privacy and data protection and surveillance (WP238), which followed on from an earlier working document (WP228) and opinion (WP215); 2015: an opinion on the question of applicable law in the digital environment, in the light of the CJEU *Google Spain* ("right to be forgotten") judgment (WP179 update), which followed on from earlier guidelines (WP225); a statement on the implementation of the *Schrems* judgment (no number); an opinion on the C-SIG Code of Conduct on Cloud Computing (WP232); an report on a "cookie sweep combined analysis" (WP229); 2014: an opinion on the application of the e-Privacy Directive to device fingerprinting (WP224); an opinion on "recent developments on the Internet of Things (WP223); a statement on the implications of the *Digital Rights Ireland* case (WP220); 2013: an opinion on obtaining consent for cookies (WP208); an opinion on apps on smart devices (WP202); 2012: an opinion on cloud computing (WP196); an opinion on cookie consent exemption (WP194); 2011: an opinion on geolocation services on smart mobile devices (WP185); 2010: an opinion on global transfers of passenger name record (PNR) data to third [i.e., non-EU/EEA] countries; etcetera.
Also important are the opinions of the European Data Protection Supervisor, which can relate to all areas of Union, i.e., both to matters addressed in the EC directives and in the instruments relating to police and judicial cooperation. They can be found here:
https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications

[49] See in particular cases C-518/07 of 9 March 2010 against Germany, C-614/10 of 16 October 2012 against Austria, and C-288/12 against Hungary.

[50] See GDPR, Chapter VI, Independent Supervisory Authorities, section 1, *Independent Status*, in particular Article 52.

[51] *Idem*, Article 57.

[52] *Idem*, Article 58 (selection). The article lists altogether 6 "investigative powers", 10 "corrective powers", and 10 "authorisation and advisory powers"; and adds to this a power "to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal

proceedings, in order to enforce the provisions of this Regulation". The EU Member States may add even further powers to all this.

[53] Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (note 34, above), Article 15, moving Article 1 of the Additional Protocol into the main text. On the required powers of the authorities, see in particular Article 15(2) and (4).

[54] Establishment of Harmonized Policies for the ICT Market in the ACP Countries, HIPCAR, Privacy and Data Protection: Model Policy Guidelines & Legislative Texts, ITU 2012, available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/privacy_and_data_protection_model%20policy%20guidelines.pdf

[55] Establishment of Harmonized Policies for the ICT Market in the ACP Countries, HIPSSA, Data Protection: Southern African Development Community (SADC) Model Law, ITU 2013, available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[56] Projets de Lois Types de la Communauté Economique des Etats de l'Afrique Centrale (CEEAC) et Projets de Directives de la Communauté Economique et Monétaire de l'Afrique Centrale (CEMAC), Cybersécurité, ITU 2013, available (in French only) at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/REGIONAL%20documents/projets_des_lois_types-directives_cybersecurite_CEEAC_CEMAC.pdf

[57] Cf. HIPCAR, Privacy and Data Protection: Model Policy Guidelines & Legislative Texts (note 53, above), Article 19(1) ("comparable level of protection"); HIPSSA, Data Protection: Southern African Development Community (SADC) Model Law (note 54, above), Article 44 ("adequate"); CEEAC/CEMAC Model Law/Directive on Data Protection (note 55, above), Article 60 ("adequate").

[58] See Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 4, above), section 3.6, *Exercise of extraterritorial jurisdiction by states*, with detailed references. See also the discussion of the ECtHR *Perrin* case and the French *Yahoo!* case in Douwe Korff & Ian Brown, *Social media and human rights*, Chapter 6 in: Human rights and a changing media landscape, Council of Europe, 2011, p. 195ff., available at: https://www.coe.int/t/commissioner/source/prems/MediaLandscape2011.pdf.
See also more generally the Internet & Jurisdiction Project: http://www.internetjurisdiction.net/
And more specifically: Bertrand de La Chapelle and Paul Fehlinger, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation, available at: http://www.internetjurisdiction.net/wp-content/uploads/2016/04/Internet-Jurisdiction-Project-Jurisdiction-on-the-Internet-by-Bertrand-de-La-Chapelle-and-Paul-Fehlinger.-Global-Commission-on-Internet-Governance.pdf

[59] Scassa, Teresa and Robert J. Currie, New First Principles: Assessing the Internet's Challenges to Jurisdiction, Georgetown Journal of International Law 42(4): 1018 (2010), quoted in Bertrand de La Chapelle and Paul Fehlinger, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation (previous note), Executive Summary.

[60] *Google Spain v. AEPD*, Case C-131/12, CJEU Grand Chamber judgment of 13 May 2014, para. 60 (where the Court applied this approach specifically to search engines and establishments linked to search engines). See also the Article 29 Working Party Opinion on the question of applicable law in the digital environment, in the light of the CJEU *Google* ("right to be forgotten") judgment (WP225). For a further discussion, see: Brendan Van Alsenoy and Marieke Koekkoek, Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the EU's "Right To Be Forgotten", 2015, available at: https://ghum.kuleuven.be/ggs/publications/working_papers/new_series/wp151-160/wp152-alsenoy-koekkoek.pdf

[61] The English version of the Directive uses the word "equipment", but other language versions – which in EU law are equally authentic – use the relevant word for "means", such as "*moyens*" (French), "*Mittel*" (German).

[62] Article 29 Working Party, Opinion 8/2010 on applicable law, adopted on 16 December 2010 (WP179), pp. 20 – 22.

[63] See Douwe Korff, Expert Opinion, prepared for the Committee of Inquiry of the German *Bundestag* into the "5EYES" global surveillance systems revealed by Edward Snowden (note 20, above), section A.2, p. 4ff.

[64] See Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 4, above), section 4.5.5, *Investigating crimes in the digital environment*, under the heading "Article 32 of the Cybercrime Convention".

[65] See: David Banisar (of the NGO Article 19), National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map, available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416
Also: DLA Piper, Data Protection Handbook, providing basic information on countries with privacy laws worldwide and also including a world map:
https://www.dlapiperdataprotection.com/#handbook/
https://www.dlapiperdataprotection.com/#handbook/world-map-section/c1_HK/c2_GB

[66] United Nations Conference on Trade and Development (UNCTAD), Data protection regulations and international data flows: Implications for trade and development, 2016, Executive Summary, p. 7, available at:
http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf
The full report is available here:
http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_summary_en.pdf

[67] Turkey was the last Council of Europe Member State to ratify the Convention, which it did on 2 May 2016. The Convention will enter into force for Turkey on 1 September 2016.

[68] UN GA Resolution 68/167 on the right to privacy in the digital age, adopted on 18 December 2013, UN Document A/RES/68/167, available at:
http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

[69] Report of the High Commissioner for Human Rights on the right to privacy in the digital age, UN Document A/HRC/27/37, 30 June 2014, available from:
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
For more general information on the UN developments, see:
http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

[70] The Special Rapporteur on the Right to Privacy presented his first report to the Human Rights Council in March 2016, which set out detailed plans to address the issues at the global level, see: Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, UN Document A/HRC/31/64, 8 March 2016, available from:
http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

[71] Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines, section on *Transborder flows of personal data*, p. 30.

[72] See the Article 29 Working Party documents on biometrics: WP29 Working document on biometrics (WP80, 2003); WP29 Opinion 02/2012 on facial recognition in online and mobile services (WP192); WP29 Opinion 3/2012 on developments in biometric technologies (WP193), all available from:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/index_en.htm

[73] See: UN Guidelines, Principle 6; OECD Guidelines, Principle 4; APEC Privacy Framework, Principle 13; Council of Europe Data Protection Convention, Article 8; EU Data Protection Directive, Article 13; EU General Data Protection Regulation, Article 23.

[74] See: Douwe Korff, Ben Wagner, Julia Powles and others, Boundaries of Law: exploring transparency, accountability and oversight of government surveillance regimes (forthcoming).

[75] *Idem*.

[76] See the selection of "cybersecurity" definitions in this handout and presentation:
https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20Handout%20-%20DK150119.pdf
https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CPDP%202015%20-%20KORFF%20presentation.pdf
The ITU defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." See:
http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[77] Note that the Council of Europe Cybercrime Convention (also known as the "Budapest Convention"), which lists many specific "cybercrimes", still leaves the states that are party to it considerable leeway in the definition of those crimes, including the exceptions to those crimes (e.g., in relation to intellectual property issues and hate crimes).

[78] But note that in reality, data in "cyberspace" are still always in some country. This is further discussed later in the text in relation to cross-border law enforcement and national security activities.

[79] See note 13, above.

[80] Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner, Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, Computer Science and Artificial Intelligence Laboratory Technical Report, Massachusetts Institute of Technology, MIT-CSAIL-TR-2015-026, 6 July 2015, available at:
https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf
The quoted text is from the Executive Summary.

[81] See again the paper and Executive Summary mentioned in the previous note. Also the European Digital Rights (EDRi), Position paper on encryption: High-grade encryption is essential for our economy and our democratic freedoms (prepared by EDRi member organisation Bits of Freedom), 7 January 2016, available at:
https://www.edri.org/files/20160125-edri-crypto-position-paper.pdf

[82] See, with particular reference to the issues in the Cybercrime Convention, Douwe Korff, The Rule of Law on the Internet and in the wider digital world (note 4, above), Section 4.5.5, *"Investigating crimes in the digital environment*".

[83] On the Reference Guide, see:
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx
As explained there, the Reference Guide is being developed in a project carried out by the ITU in partnership with the CCI, CTO, ENISA, GCSP, GCCC University of Oxford, Microsoft, NATO CCDCOE, OECD, OAS, UNCTAD and World Bank.
The National Cyber Security Strategy (NCS) Toolkit can br found here:
http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf

[84] See:
http://www.oxfordmartin.ox.ac.uk/cybersecurity/

[85] See:
http://www.thegfce.com/

[86] The starting point for the latter could be the "*'intelligence codex' addressed to the intelligence services of all [Council of Europe Member States], which lays down rules governing co-operation in the fight against terrorism and organised crime*", recommended by the Parliamentary Assembly of the Council of Europe (PACE) in its Recommendation on Mass Surveillance, Recommendation 2067 (2015), 21 April 2015, para. 2.3, available at:
http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21694&lang=en
However, rather than only addressing "co-operation", it should also set standards and limitations on what the agencies may and may not do, even purely domestically. That could be done indirectly, by such a "codex" stipulating that state agencies should not co-operate with agencies of other states unless those other agencies were subject to such standards and limitations – but it would be better stipulated directly.

[87] See: http://ec.europa.eu/trade/policy/in-focus/ttip/index_en.htm

[88] See: http://ec.europa.eu/trade/policy/in-focus/ceta/index_en.htm

[89] See: https://ustr.gov/tpp/

[90] For an overview of the criticisms, in particular in relation to digital rights (including not just data protection but also copyright and net neutrality, etc.), see the EDRi booklet, TTIP and digital rights, available at:
https://edri.org/files/TTIP_and_DigitalRights_booklet_WEB.pdf

[91] ITU data, 2015.

[92] For an overview, see Chris Hoofnagle, *Country Study – United States of America*, produced as part of a major study for the European Commission, New Challenges to Data Protection, 2010, available at:
http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b1_usa.pdf

[93] UNCTAD, Data protection regulations and international data flows: Implications for trade and development, 2016, Executive Summary (note 66, above), p. 7. Point re-ordered.

[94] See the list of powers that must be granted to the data protection authorities under the GDPR, summarised in Part 2, at the end of sub-section 2.4.3.

[95] UNCTAD, Data protection regulations and international data flows: Implications for trade and development (note 66, above), Executive Summary, p. 7.

[96] On the Article 29 Working Party and these recommendations etc., see note 48, above. On the new EDPB, see the GDPR, Chapter VII, Section 3, Articles 68 – 76. The Board's independence is addressed in Article 69.

[97] EU Fundamental Rights Agency, Data Protection in the European Union: the role of National Data Protection Authorities (a second report by the FRA on "Strengthening the fundamental rights architecture in the EU"), 2010, available at:
http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

[98] *Idem*, Executive Summary, p. 7.

[99] See Douwe Korff, Ben Wagner, Julia Powles and others, Boundaries of Law: exploring transparency, accountability and oversight of government surveillance regimes (note 74, above), section 2.3.3, *Untargeted generic access ("mass surveillance")*, at (d) Formal requirements and (f), Oversight.

[100] Original Explanatory Memorandum to the OECD Privacy Guidelines (1983), p. 43.

- o – O – o -