THE INTERNET

A GLOBAL FREE SPACE WITH LIMITED STATE CONTROL

No. 92, November 2014

ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS
ADVIESRAAD INTERNATIONALE VRAAGSTUKKEN

AIV

Members of the Advisory Council on International Affairs

P.O. Box 20061
2500 EB The Hague
The Netherlands

telephone + 31 70 348 5108/6060
fax + 31 70 348 6256
aiv@minbuza.nl
www.aiv-advice.nl

Members of the Combined Committee on Internet Freedom

Chair	Professor Egbert Dommering
Members	Dr Bibi van Ginkel
	Professor Marieke de Goede
	Professor Bert-Jaap Koops
	Dr Elly Plooij-van Gorsel
	Heikelina Verrijn Stuart
Executive Secretary	Jantinus Smallenbroek

This advisory report is based on texts and drafts drawn up for this purpose by the chair and members of the preparatory committee or taken, with their consent, from their previous academic publications. These may also form part of their future publications.

Contents

Foreword

I Introduction 7

II Brief history of modern telecommunications: the origins of the internet 11

II.1 The establishment of the national utilities (PTTs), united in the International Telecommunication Union 11

II.2 The technical organisation of the internet, the World Wide Web and the role of classical international organisations and national states 14

II.3 Other forums which are (or wish to be) involved in the organisation and control of the internet 16

II.4 Role of national states: access to the internet and control of the private access providers 19

III Conceptual issues: privacy, freedom and fundamental rights 20

III.1 The system of fundamental rights shaken up 20

III.2 Specific privacy issues 24

III.3 The internet and freedom of expression: new intermediaries, blurring of distinction between public and private, commercialisation of the public sphere and mobilisation 29

III.4 The relationship between legal concepts, technology and sovereignty 30

III.4.1 Law and technology: privacy of communication, traffic data, security and intermediaries 31

III.4.2 National sovereignty: jurisdiction and fundamental rights violations 33

IV The main legal frameworks 35

IV.1 The UN 35

IV.2 The Council of Europe 36

IV.2.1 The Committee of Ministers and the Parliamentary Assembly 36

IV.2.2 The European Court of Human Rights 36

IV.3 The European Union 40

IV.3.1 General 40

IV.3.2 The EU and privacy 42

V Four categories of issues 46

V.1 The multistakeholder model and the roles that states, the private sector and NGOs can play in internet governance 46

V.2 The dilemmas facing the Western democracies: the United States and the Netherlands 51

V.2.1 The United States 51

V.2.2 The Netherlands 55

V.3 Censorship, control and the mobilising function of the internet 59

V.4 The role of the private sector 62

VI Summary, conclusions and recommendations 64

Annexe I Additional information about the history of current telecommunications

Annexe II (a) Request for advice

Annexe II (b) Resolution: 'The right to privacy in the digital age'

Annexe II (c) International Principles on the Application of Human Rights to Communications Surveillance

Annexe III List of abbreviations

Annexe IV List of persons consulted

Foreword

On 20 February 2014 the government asked the Advisory Council on International Affairs (AIV) to produce an advisory report on internet freedom. The request singled out the rights to privacy, data protection, confidential communication and freedom of expression as notable examples of internet freedom. The basic principle of internet freedom is that fundamental rights that exist offline should also apply online. The creation and rapid growth of the internet have spawned new forms of communication, which have in turn raised new questions about how these rights can be safeguarded, particularly since they must sometimes be balanced against security interests. The government asked the AIV how internet freedom could continue to be promoted in Dutch domestic and foreign policy, how far Dutch jurisdiction extends and what role should be played by the private sector in promoting internet freedom. The request for advice is contained in annexe II to this advisory report.

To prepare this advisory report the AIV established a combined committee chaired by Professor Egbert Dommering (member of the Human Rights Committee). The other members of the combined committee were Dr Bibi van Ginkel and Professor Marieke de Goede (members of the Peace and Security Committee), Professor Bert-Jaap Koops (member of the Human Rights Committee), Dr Elly Plooij-van Gorsel (member of the AIV/European Integration Committee) and Heikelina Verrijn Stuart (member of the AIV/Human Rights Committee). Simone Halink (Ministry of Foreign Affairs) was involved in the preparation of the report as civil service liaison officer. The committee was assisted by Jantinus Smallenbroek (executive secretary) and Sophie Meijer and Lisan Warnier (trainees). In the course of preparing the report the committee consulted the following experts: Caspar Bowden (independent privacy researcher), Dr Quirine Eijkman (head of Political Affairs & Press Office at Amnesty International Dutch Section), Hielke Hijmans (head of Policy & Consultation Unit at the European Data Protection Supervisor (on sabbatical leave)), Professor Erik Huizer (CTO at SURFnet and professor of internet applications at Utrecht University), Professor Milton Mueller (professor at Syracuse University School of Information Studies) and Rejo Zenger and Hans de Zwart (both with the Dutch digital rights organisation Bits of Freedom). The AIV is grateful to them all for sharing their views.

The AIV finalised this report on 1 December 2014.

I Introduction

The request for advice states that the concept of internet freedom consists of a number of rights and freedoms that have been enshrined in international conventions for many decades. The subject of internet freedom therefore relates not to new rights and freedoms but to existing rights and freedoms seen through the prism of the internet.

The internet has created a society that is less restricted by national borders than ever before. It has wrapped society in an electronic net, which uses the universal standard (the Internet Protocol) and the World Wide Web (www) to connect everyone and everything: people with people, people with knowledge sources, people with public and private sector organisations and people with things. This is being done in an individualised manner which has no parallel in human history. The capacity of fixed and mobile, interconnected electronic networks has increased enormously in the past decade. Accessibility has become more and more universal and less and less tied to a fixed location. Owing to the huge computing and storage capacity of computers, it has become possible to distil behavioural profiles of individuals and groups from individual human actions and connections which leave traces on the internet. These profiles can be used for the purposes of commerce (marketing), government (welfare services) and state security (counterterrorism). Big data has become a buzz word at the start of the twenty-first century, just as Big Brother was in the second half of the twentieth century. Processing huge quantities of data is a task that faces every branch of science and is in danger of becoming a goal in itself.[1] It makes use of techniques such as data mining and the interlinking of large databases. This makes it possible to build profiles and expose links. A database can consist of not only content data but also (in the context of electronic communication, which is the subject of this report) traffic data: i.e. data used for handling electronic communications (transport and invoicing). Far-reaching conclusions can be drawn from the patterns of relations exposed between traffic data. Nowadays, it is more important to analyse traffic data than to intercept communications to discover the content.

The positive side of the internet (and of the wealth of services and applications available on it) is the huge boost it gives to prosperity and to individual opportunities for personal development, the development of knowledge and new economic activities and, above all, the unprecedented transparency of niche markets. The negative side is that never before in human history have large commercial, government and military organisations been able to wield so much power over individuals and groups. This power often extends beyond national borders and is usually invisible. The new term for this phenomenon – behavioural targeting – has already gained wide currency, albeit mainly in a marketing context. It should be noted, by the way, that the positive aspects of the internet can sometimes be overestimated. The internet has led to the concentration of power in the communications sector. And transparency has also caused destructive unbundling processes and the undermining of quality standards in the market.

The AIV itself interprets the concept of internet freedom as the organisation of free and equal accessibility to and free (unmonitored) public and non-public communication on

1 See the wide-ranging analysis of the German philosopher of science Klaus Mainzer, *Die Berechnung der Welt, Von der Weltformel zu Big Data*, Munich: C.H. Beck, 2014.

the internet, both between people and between people and the services available on it. This therefore includes both public and private communication. The request for advice puts rather more emphasis on the latter. The AIV will explain in chapter III that the internet has blurred the distinction between these two forms of communication. Both forms will be analysed, but the emphasis will be on private communication, in keeping with the request for advice.

The internet is an open network which is prey to attacks that can jeopardise national and individual freedom. The AIV trusts that this advisory report can help to strike the right balance between proportionate measures to prevent such attacks and the forms of free and lawful use guaranteed under the rule of law.

Parameters for norms and freedom

The norms that apply to the internet form a very complex system. The norms can be of a legal or a non-legal nature. And they can be of a national or international origin or come from some other source. The politicologist Joseph Nye has designed an illuminating model for this purpose.[2] The model evaluates the strengths of the various norms by reference to four criteria:

- depth: the hierarchical coherence of a set of rules or norms in a given domain;
- breadth: the number of actors that have accepted the norms;
- fabric: the mix of state and non-state actors subject to the norms and the degree to which relations between them have been put on a formal footing;
- compliance: the degree of behavioural adherence to the norms.

In technical terms, the structure of the internet is very loose and the norms are informal (i.e. little depth and a loose fabric), but it scores highly in terms of compliance, because all parties have an interest in maximum interconnectivity and hence in enforcing standards (i.e. much breadth and a high rate of compliance). The non-state origin of the internet is therefore conducive to the quality of compliance. A factor not included in Nye's system but nonetheless considered by the AIV to be important is that the internet community still stands for a shared system of norms and values conducive to social cohesion (compliance). The internet scores poorly for cybersecurity because access is very open, the diversity of users is very great (certainly in the case of non-state terrorism and other illegal activities) and the consistency and transparency of the set of norms are low. This is the crux of the issue that has come to be known as internet governance.

The values associated with the concept of internet freedom are based on the categories used by Freedom House in its reports measuring the level of internet and digital media freedom on a country-by-country basis. The categories are as follows:[3]

- obstacles to access: infrastructural and economic barriers to access (sometimes via other measures not based directly on the internet), governmental efforts to block

2 Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance Paper Series, no. 1, May 2014. See: <http://www.ourinternet.org>.

3 Freedom House, *Freedom on the Net 2013*, see: <http://freedomhouse.org/sites/default/files/resources/ FOTN%202013_Full%20Report_0.pdf>, p. 16, consulted on 1 September 2014.

specific applications and legal, regulatory and ownership control over internet access providers;
- limits on content: statutory provisions regulating content, technical filtering and blocking of websites, self-censorship, the diversity of online news media and the role of digital media for social and political activism;
- violations of user rights: legal protections and restrictions on online activity, surveillance, privacy and repercussions for online activity, such as legal prosecution, imprisonment or physical intimidation.

However, the model views the internet solely from the perspective of freedoms and disregards its significant role in the economy. A country such as China, which scores badly in the Freedom House reports, grants substantial internet freedom for commercial and non-political communication.

Scope of the advisory report

The concept of *cybersecurity* has various meanings. First, it can relate to measures taken in respect of internet access and use to minimise the risks of fraud, terrorism and other criminal activities. The term can also be interpreted in a broader sense as meaning the protection of fundamental values which could be compromised by an unsafe internet. The AIV has dealt with these aspects in more detail in its advisory report 'Cyber Warfare'.[4] Although the subjects of cybersecurity and cybercrime overlap with internet freedom in some ways, they are not dealt with here at greater length because of the need to limit the scope of this report. The subject of this report is how – given the ongoing need to combat terrorism – the achievements of the rule of law and the rights and freedoms they confer can be safeguarded and how the Netherlands can play a leading role. The question arises of how any restrictions of fundamental rights can fulfil the requirements of being proportionate and prescribed by law and of providing effective legal protection against interference. Although the current perception is that the threat is permanent and that the internet plays a crucial role,[5] this must not result in permanent surveillance of all citizens and untargeted data collection. In such a situation it is of crucial importance to safeguard and continue to develop the legal frameworks and protect civil liberties.

Nowadays, free access to the internet is associated (at any event in the Netherlands) with the concept of network neutrality. As this subject is closely related to (European) competition law, the AIV will not consider it in this report.

The internet is increasingly the scene of a clash between conflicting rights such as freedom of expression, privacy and copyright. Although these clashes naturally have a bearing on the concept of internet freedom as defined above, they will only be touched on in passing in this report as they fall outside the committee's remit. This is also a problem which is first and foremost a matter for the courts.

4 Advisory Council on International Affairs and Advisory Committee on Issues of Public International Law, *Cyber Warfare*, advisory report no. 77 (AIV)/no. 22 (CAVV), The Hague, December 2011.

5 General Intelligence and Security Service, *Online Jihadism important driving force behind global Jihad movement*, January 2012. See: <https://www.aivd.nl/@2872/jihadistisch/>.

Structure of the report

Chapter II gives a very brief outline of the history of telecommunications (the origin of the internet) and how the internet is presently organised. A more detailed explanation can be found in annexe 1. This subject deserves special attention since the internet is a successful example of international governance in which participation is not restricted solely to multilateral organisations and states, but also extends to stakeholders. As it also involves a loosely structured and non-hierarchical system of groups, this form of governance can also be described as a multi-agent system.[6] Indeed, it is probably one of the most successful examples of such a system. Chapter II goes on to outline the efforts made by some states both now and in the past to impose a classical international system of governance on the internet. They have also attempted to stretch the concept to include all kinds of content-related matters. Finally, chapter II examines what parts of the internet come within the national sphere of influence.

Chapter III analyses how the conceptual framework of communication- and privacy-related fundamental rights that has taken shape in a physically visible world must be rethought in the world of cyberspace. This is necessary because rights that were previously conceptually separate have become increasingly intertwined. Chapter III also shows how legal concepts are becoming increasingly divorced from the underlying reality and how the role of the traditional cornerstone of public international law – the sovereign state – is undergoing fundamental change.

Chapter IV briefly discusses the relevant international law frameworks, with particular reference to the problems we are considering here.

Chapter V examines four categories of issues relevant to internet freedom and how each of them requires its own approach. Finally, chapter VI contains a summary and sets out conclusions and recommendations.

6 For a description of the multi-agent approach, see Luciano Floridi, *The 4th Revolution*, *How the Infosphere Is Reshaping Human Reality*, Oxford: Oxford University Press, 2014, chapter 8: 'Politics: the rise of the multi-agent system'.

II Brief history of modern telecommunications: the origins of the internet

This chapter explains how the structure of telecommunications (nowadays referred to as electronic communications)[7] has changed, due in part to the advent of the internet, with state monopolies giving way to a system that has evolved organically. The organisations that form this system are not part of any kind of hierarchy. Nor are they tied to states, although some have a loose connection with the United States. Control over telecommunications is therefore spread more diffusely than in the past. Further information can be found in annexe 1.

II.1 The establishment of national utilities (PTTs), united in the International Telecommunication Union

At the end of the nineteenth century the European countries and the United States started to build a landline telephone network within their national borders. The United Kingdom led the way in establishing a worldwide telegraph network, linking the countries of the Commonwealth. The European model centred on the state-owned enterprise, which was also assigned important utility functions such as ensuring that the entire population was connected to the telephone network at an affordable price (known as the universal service). These state-owned enterprises obtained a monopoly within their national territory because constructing physical infrastructure in unprofitable areas was part of their task as a public utility. The same model was adopted *de facto* in the United States because AT&T's monopoly was respected as long as the company rolled out the physical infrastructure throughout the entire country. These utility monopolists were vertically integrated companies which controlled the entire supply chain up to and including the peripheral equipment through which consumers obtained the service. This telephone, telegraph and telex monopoly was usually added to the existing postal monopoly (hence: 'PTT', the post, telephone and telegraph combination).

The first half of the twentieth century saw a great leap forwards towards wireless communication using radio frequencies. In so far as radio frequencies were used for PTT services, they were allocated to the existing utility monopolists. However, where the frequencies were used for the newly emerging mass broadcasting medium they were assigned to oligopolistic structures (as in the United States) or to separate utility companies, which managed them for the benefit of the broadcasting organisations.

International telephone traffic (the coordination of rates and standards) and the orderly use of frequencies (the linking of frequencies to certain services) required a stable international legal framework and consultation structure. The International Telegraph Union, the forerunner of the International Telecommunication Union (ITU), was founded for this purpose in 1865. This led to the formation of a service-based and state-linked pyramid-style structure. Before long a distinction was made between what is usually described for the sake of brevity as 'content' and 'transport'. The post, telegraph and telephone services (PTTs) dealt with transport and related services only.

7 Electronic communications is the term used in European legislation for what is still known in common parlance as telecommunications, i.e. voice telephony and the internet.

New spatial infrastructure

The first major departure from this self-contained pyramid-style model came with the building of a satellite infrastructure in the 1960s and 1970s. The first commercial satellite – the Telstar – was launched in 1962. Although states retained a monopoly on earth services (the allocation of frequencies to the satellite earth station), the range of the satellites bore little relation to national borders. This broke the state monopoly and created the various divides, spelled out below, not only in the international telecommunication world but also in the broadcasting world, where it had been customary to use technical standards and legal devices such as copyright to shield national territories.

The first divide was between East and West: authoritarian states such as Russia and China demanded that foreign satellite signals should not be beamed at their territory. This sparked what was known as the satellite controversy in the UN, which pitted those in favour of a prior consent regime against advocates of the free flow of information. Ultimately, a compromise provision was adopted by the World Administrative Radio Conference for inclusion in the ITU's Radio Regulations. Under this provision, the members would use all technical means to avoid beaming the signal at a foreign territory, unless agreement had previously been reached with the receiving state. This seems to be a victory for the prior consent principle. In practice, however, some 'spillover' is technically unavoidable. It follows that the provision actually legalises a situation where a satellite signal can be received in the territory of a foreign state. For the most part, therefore, satellite signals were receivable outside the territory at which the signal was directed, even if no consent had been obtained.[8]

Another departure from the self-contained national system concerned the prior consent provision. This provision had been intended for direct broadcasting, in other words a system in which satellites broadcast to the general public on a waveband intended for the broadcasting organisation. Gradually, however, the telecommunication satellites intended for individually addressed signals also came to be used for broadcasting purposes. This blurred the distinction between direct-broadcasting satellites and telecommunication satellites. The latter came to be increasingly used for broadcasting purposes, particularly by commercial satellite organisations. Originally, this was viewed as illegal since the signals were secret and therefore not intended for the public at large. Ultimately, however, the free flow of information principle triumphed. According to this principle, social use and not the technical definition is decisive.[9] This was the first step towards uncoupling services from their intended infrastructure, which would later be a characteristic of the internet as well. The present debate about the international governance (and scope of governance) of the internet can be seen as a revival of the East-West debate. This debate will forever be associated with the famous 1980 MacBride report entitled 'Many Voices, One World' on communication problems in modern societies.[10]

8 For the history of this international debate, see J.E.S. Fawcett, *Outer Space, New Challenges to Law and Policy*, Oxford: Clarendon Press, 1984.

9 Autronic AG v. Switzerland, ECtHR, 22 May 1990, Series A, vol. 178.

10 See: <http://unesdoc.unesco.org/images/0004/000400/040066eb.pdf>.

The second divide involved the North-South controversy about the ownership of scarce resources. Satellites use the geostationary orbit over the equator, ownership of which was claimed by the African countries. This claim was never honoured. The debate on scarce resources and the disadvantaged position of the developing countries still dominates the North-South electronic communication debate. And the divide is as sharp as ever. It follows that the absence of properly developed physical infrastructure is the main internet freedom issue in developing countries. As this subject is not part of the committee's remit, it will receive no further consideration here.

The construction of the cable network in various European countries and in the United States meant that satellite broadcasting obtained an easy alternative landing site in the national states. This also acted as the lever for liberalisation of the broadcasting market. Until then, the market had been dominated by public broadcasting organisations, particularly in Europe.

Data, digitalisation and demonopolisation

Various trends that can be called the three Ds – data, digitalisation and demonopolisation – are coming together on the internet.

In the 1970s and 1980s new telecommunication markets were developed on both sides of the Atlantic, particularly for digital data services.[11] The switch from speech to data began in the 1980s. The institutional and commercial users of the telecommunication network and telecommunications services had a growing need for data storage and distribution systems that would allow commercial messages to be transmitted and stored quickly and efficiently. An example was alphanumeric communications, such as fund transfers between banks. The PTTs responded by developing, within their utility monopoly, a data service with which they hoped to service this new market and tie the computer manufacturers to their standards. However, the liberalisation of the fixed infrastructure made it possible for more and more alternative data applications to be developed on the networks of institutions and businesses. The best-known initiative was that of the US government, which needed an efficient and safe data network. Acting for the defence organisation ARPA, the university community developed protocols for the transmission of messages and data over an electronic network: i.e. the Internet Protocol (IP), the Transmission Control Protocol (TCP) and the Datafile Transfer Protocol (DTP). In the ensuing battle of the standards, the protocol developed by the PTTs eventually lost out worldwide to the much simpler TCP/IP protocol.[12] With the support of the US National Science Foundation, this gradually evolved into a commercial, worldwide open network which supplanted the applications developed by the PTTs. In 2001, during the development stage, a period of what economists term 'creative destruction' occurred. This is a crisis which not only destroys but also generates fresh impulses,[13] and is followed by innovative growth as well as further commercialisation and attempts

11 See Manuel Castells, *Communication Power*, Oxford: Oxford University Press, 2009, chapter 2, 'Communication in the digital age'.

12 For a detailed analysis of this trend see Janet Abbate, *Inventing the Internet,* Cambridge: The MIT Press, 1999, chapter 5, 'The internet in the arena of international standards'.

13 Carlota Perez, *Technological Revolutions and Financial Capital, The Dynamics of Bubbles and Golden Ages*, Cheltenham: Edward Elgar (EE), 2002.

to appropriate the network for its own purposes. This period saw the birth of such corporate giants as Google, Facebook, Twitter and Netflix.

The technical features of the internet make it a platform for every service presented in accordance with the correct standards. The TCP/IP protocol makes every service independent of the infrastructure and thus guarantees universal end-to-end connectivity for all services provided in accordance with the protocol. The end-to-end principle means that intelligent applications not related to transport are kept off the network. The same development has occurred with computers: the software can now function on all hardware and vice versa. Moreover, the liberalisation of the electronic communication market has provided access to the network for services that compete with the network operator. Besides hosting a wide range of services for short messages (from email to Twitter), the internet has powerful applications (through the World Wide Web) of web browsers and search engines capable of searching the entire network and making documents, images and audio accessible worldwide (for example through Google and YouTube).

II.2 The technical organisation of the internet, the World Wide Web and the role of classical international organisations and national states

The internet has been shaped outside the ITU frameworks and is mainly based on private law agreements and voluntary cooperation. No hierarchical relationship exists between most internet organisations, although there are overlapping memberships. Despite the fact that many different parties are involved in developing the internet and keeping it operational, the internet functions well as a platform for the applications running on it, such as browsers, search machines, the World Wide Web, email and many others.

The technical structure of the internet has emerged from what can broadly be described as the internet community, a collection of clubs partly originating from academia.[14] One of the internet's pioneers, David Clark, formulated the anarchist principle of governance in the following terms in 1992: 'We reject presidents, kings and voting. We believe in rough consensus and running code.'[15] What he meant was that internet governance involved a universal code (the Internet Protocol) about which there was broad agreement, thereby guaranteeing the end-to-end principle. This universally acknowledged need for consensus on technical standards is the driving force behind the internet community, however complex it may be. This is also the view taken by Joseph S. Nye, who was quoted in the introduction.[16]

1992 saw the founding of the Internet Society (ISOC), which is still active. ISOC was intended to be the intellectual centre of the internet, with a pivotal role being played by people such as Vint Cerf (another internet pioneer). ISOC was intended to coordinate all the different groups informally working together, which mainly derived their authority from

14 For a history of the formation of internet governance, see Milton Mueller, *Ruling the Root*, Massachusetts: Massachusetts Institute for Technology, 2002.

15 Idem, note 11 on p. 91.

16 Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance Paper Series, no. 1, May 2014. See: <https://www.ourinternet.org>.

that of the individuals who worked for them.[17] ISOC still serves as a legal umbrella for those involved in developing standards.

In the early 1990s, there was still no more than a fairly loose structure, with the internet community consisting of US government and academic organisations and the US Department of Defense. However, all this changed with the advent of the World Wide Web, the graphical shell which radically changed internet navigation and heralded the breakthrough of the internet to the public at large and the market. Domain names established a link between the internet and protected trademarks and other commercial distinguishing marks. Domain names therefore acquired great commercial value. As a result, businesses and international organisations such as the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO) obtained a stake in the internet. This situation led to the institutionalisation of control over the root, which is the address system linking domain names with IP addresses. This process resulted in the establishment of the Internet Corporation for Assigned Names and Numbers (ICANN), which is a compromise between the internet community and advocates of more traditional interests.

The history of the Internet Corporation for Assigned Names and Numbers (ICANN)

The discussion concerned the extent to which the Domain Name System (DNS) should be incorporated into the American regulatory system. ICANN was established following a fairly intensive lobbying process. This was supported by what was known as a 'dominant coalition' of stakeholders, in which old and new players united to challenge the efforts by the US authorities to keep the DNS within the American sphere of influence. In 1998, however, the Clinton administration announced in a White Paper that it was prepared to enter into a contract on the DNS with a non-profit organisation, which would be established in the United States and have an international management board to administer the DNS. The White Paper invited proposals by stakeholders. A compromise therefore had to be found between the US authorities, internet societies, major companies such as IBM, lobbying organisations of trademark proprietors, the European Commission and foreign governments (in particular Australia, France and Japan). The organisation would have to be built around the informal structure for the assignment of internet addresses – the Internet Assigned Numbers Authority (IANA). The legal form chosen was that of a non-profit corporation under Californian law. This legal form is often used in the United States for charitable and educational institutions. In late 1998 ICANN and the US Department of Commerce concluded a Memorandum of Understanding, which ultimately led to the present structure.

ICANN has a Joint Project Agreement and a contract with the US Department of Commerce for the assignment of internet addresses and the management of generic top-level domains (gTLDs). The US Department of Commerce, together with the Governmental Advisory Committee (GAC), is therefore the formal link with the authorities. Unlike the US Department of Commerce, the GAC has no legal authority to act on behalf of governments.

17 Milton Mueller, *Ruling the Root*, Massachusetts: Massachusetts Institute for Technology, 2002, p. 94.

The structure of ICANN has been described as 'baroque in its complexity', reflecting the broad range of interests affected by domain name policy.[18] The Internet Engineering Task Force (IETF, see annexe I) and similar organisations have delegates on ICANN's committees, but they do not form part of it. All these organisations are autonomous. As there is no hierarchical relationship between them, this does indeed constitute a multi-agency model in which multiple stakeholders are represented.[19]

The Joint Project Agreement has been repeatedly extended and amended and has gradually increased ICANN's autonomy, although the Department of Commerce retains a supervisory role.[20] In the Affirmation of Commitments concluded between the Department of Commerce and ICANN on 30 September 2009 the Joint Project Agreement was extended for an indefinite term.[21] The US Department of Commerce evolved into a kind of process monitor. All stakeholders could live with this, but the link between ICANN and the United States has become untenable as a result of the Snowden affair (on this subject see also section V.2.1).

II.3 Other forums which are (or wish to be) involved in the organisation and control of the internet

Various countries are trying to increase state control of the internet by bringing its governance under the authority of multilateral organisations, in which non-state actors have no voting rights. The discussion on the governance of the internet is presently taking place in various forums, both within the UN and elsewhere. The main UN forums are the World Summit on the Information Society, the Internet Governance Forum and the ITU. In addition, discussions are being held on the normative frameworks for the use of the internet, for example in the UN General Assembly and in the UN Human Rights Council. In these discussions the term internet governance is also used and is often given a wider meaning than the technical organisation of the internet.

The World Summit on the Information Society[22]

In 1998 a resolution was passed during the ITU's Plenipotentiary Conference on the desirability of holding a World Summit on the Information Society (WSIS). The aims included creating a better understanding of the information society, drawing up a strategic plan of action for this purpose and identifying the roles of the various partners in establishing the information society. In 2001, the UN General Assembly passed

18 L.B. Solum, *Models of internet governance*, pp. 59-60, see: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136825>, consulted on 6 June 2014.

19 Luciano Floridi, *The 4th Revolution, How the Infosphere is Reshaping Human Reality*, Oxford: Oxford University Press, 2014, chapter 8: 'Politics: the rise of the multi-agent system'.

20 Lee A. Bygrave and others, 'The naming game: governance of the Domain Name System', in: Lee. A. Bygrave and Jon Bing, *Internet Governance, Infrastructure and Institutions*, Oxford, Oxford University Press, 2009, pp. 151-153.

21 See: <http://www.ntia.doc.gov/page/docicann-agreements>, consulted on 5 June 2014.

22 Amanda Hubbard, Lee A. Bygrave, 'Internet governance goes global', in: Lee A. Bygrave and Jon Bing, *Internet Governance, Infrastructure and Institutions*, Oxford, Oxford University Press, 2009, pp. 213-235. See also Milton L. Mueller, *Networks and States*, The MIT Press, Cambridge, Massachusetts, 2010, pp. 55-80.

a resolution on holding a summit, which ultimately resulted in the holding of a 'two-phase summit'. The first phase of the summit was held in Geneva in 2003 and was attended by some 11,000 people, including approximately 50 heads of state and heads of government. The other participants were representatives of governments, international organisations, non-governmental organisations, corporate entities and the media. The agenda was very wide-ranging and included the challenges of establishing the information society and providing access to it, ensuring freedom of expression and addressing the issue of internet governance. Various countries also raised the subject of the US control of ICANN. Two outcome documents were produced by the summit: a declaration of principles and a plan of action. The declaration of principles says, among other things, that the policy authority for internet-related public policy issues is the sovereign right of states, that the private sector has an important role in the development of the internet in both the technical and the economic fields, that civil society has an important (but unspecified) role in internet matters, and that international organisations have a facilitating role in coordinating internet-related public policy issues and developing internet-related technical standards. The declaration of principles thus assigns specific roles to various actors.

During this first phase of the summit the participants failed to reach agreement on issues of substance, including a definition of internet governance. The main point is that there were countries which wished to have a greater say in the content of the internet. This would have involved abandoning the old distinction between content and transport. However, a majority wished to retain this. The UN Secretary-General was therefore requested to set up a Working Group on Internet Governance (WGIG). The WGIG report was published shortly before the second phase of the WSIS, which was held in Tunis in 2005.[23]

Once again it proved extremely difficult in Tunis to reach agreement about issues of content. The discussions centred around ICANN. A group of developing countries supported the WGIG's proposal to transfer ICANN to a UN agency. This would mean that only states would have voting rights. The United States indicated that it would be reluctant to relinquish its historical role in the management of domain names. The EU pressed for a new oversight mechanism for ICANN. The WSIS in Tunis produced two outcome documents: the Tunis Commitment and the Tunis Agenda for the Information Society. This included a request to the UN Secretary-General to convene a new forum for multistakeholder policy dialogue: the Internet Governance Forum (IGF). The IGF is a forum in which the dialogue between governments, business entities, civil society and intergovernmental organisations can be continued, but which is itself unable to take any binding decisions and has no oversight function.

The Internet Governance Forum

The IGF has evolved into an important forum in which representatives of stakeholders and the internet community try to reach consensus on the principles of internet governance. This developing consensus is recorded in reports such as the report of the meeting in Baku (Azerbaijan) in 2012.[24] The breakdown of participants by stakeholder group at the meeting was as follows: civil society 33%, internet community 10%, national

23 See: <http://www.wgig.org/docs/WGIGREPORT.pdf>.

24 See: <http://www.intgovforum.org/cms/documents/publications/177-igf-2012-baku-internet-governance-for-sustainable-human-economic-and-social-development/file>.

governments 26%, intergovernmental organisations 6%, private sector 17% and media 8%. The ninth conference was held in Istanbul in September 2014. The problem of widely differing norms and values as identified by Nye is an obstacle to reaching consensus on non-technical issues.

The International Telecommunications Union

One of the subjects of negotiation during the ITU World Conference on International Telecommunications in Dubai in December 2012 was a new version of the International Telecommunications Regulations (ITR). The proposal for amendment and the five related resolutions have been signed by most Asian and Arab countries but few Western countries. The position of the countries of South America and sub-Saharan Africa is less clear-cut. The Western countries objected to the proposal because it also covered access to and communication on the internet. The ITU's attempt to extend the post and telephony model to the internet therefore seems to have failed. Nonetheless, the ITU will continue its attempts since its position as an international organisation that has no authority over the internet means that it is in danger of losing its raison d'être. For authoritarian countries such as Russia and China, the ITU is a possible way of modelling the structure of the international internet on the strict systems for controlling the content of the internet that apply in their own countries.

World Wide Web Consortium (W3C)

The internet (i.e. the technical infrastructure) must be distinguished from the World Wide Web, with which it is sometimes confused. What they have in common is that states and pressure groups seek to exercise control over both. The World Wide Web, which was conceived by Tim Berners-Lee in the early 1990s, created a new mass medium.[25] It was mainly as a result of this public use that the domain name system acquired a strong trademark role. This new distinguishing role led to a clash with the existing system of trademark rights.

The growing economic significance of the domain names meant that the issue of coordination and allocation became increasingly pressing. All stakeholders entered the fray: the United States and European governments, the 'internet world' and the 'old' telecommunications world of the trademark proprietors. The recent, protracted discussions about the new generic top-level domains are a repeat of this debate.

The W3C was founded to promote the (technical) development of the World Wide Web, for example by adopting standards. It is not incorporated, and operates instead under the flag of four academic institutions. Membership is open to every organisation and every individual. The majority of members are businesses, academic institutions and government bodies, which pay membership dues. Tim Berners-Lee, the inventor of the World Wide Web, is still director of W3C.

25 Tim Berners-Lee, *Weaving the Web*, New York: Harper Collins, 1999; for a detailed analysis of the trademark function, see also M.L. Mueller, *Ruling the Root*, Massachusetts: Massachusetts Institute for Technology, 2002, chapter 8.

II.4 Role of national states: access to the internet and control of the private access providers

National states retain influence, through the physical infrastructure, over user access to the internet and over the activities of service providers operating – at least in part – in their national territory. They can try to exert influence by stipulating – either through legislation or informal arrangements – that the conditions governing internet access and the extent to which the network can be tapped meet certain requirements. This is also the basis of what has come to be known as the 'renationalisation' or 'Balkanisation' of the internet: the tendency for the internet and the World Wide Web to splinter into regional or national areas in which states or groups of collaborating states hold absolute sway. In this way, binding political decisions and court judgments in national jurisdictions can compel global service providers to adapt their services to the region or national area. Google, for example, is already doing this voluntarily. The search results differ by language, country or region. This gives rise to wider questions about whether companies such as Google and Facebook, which operate internationally and have dominant positions in their markets, are evading national jurisdictions. Whatever the case, they have become essential links in the worldwide communication process.

The starting and finishing points of the internet lie within the sphere of influence of national and regional jurisdictions owing to the influence which states have over the physical infrastructure. This enables states to put their legal and political stamp on the use of the internet. It is also the source of conflicts about jurisdiction and standards, as reflected, for example, in the Snowden affair. This gives authoritarian states the power to control individual communications, regulate websites and blogs and impose various kinds of censorship.

III Conceptual issues: privacy, freedom and fundamental rights

The request for advice states that the rights to privacy, personal data protection, confidential communication and freedom of expression are examples of internet freedom. This chapter explains these concepts and examines related conceptual issues.

III.1 The system of fundamental rights shaken up

The right to respect for privacy

The right to respect for private life (privacy) has many facets and protects all aspects of citizens' private lives. These range from protection of the intimacy and freedom of one's own surroundings, the right to inviolability of the home (spatial privacy) and integrity of the body and the right to family life and protection of communication (relational privacy) to all information relating to the person (information privacy).[26] It is merely noted here that much of what is said below about the merging of rights also applies to spatial privacy. The advent of powerful information technology means that the walls of the home have become transparent and that even the most intimate aspects of private life are no longer confined within them. At the same time, information about individuals is no longer kept in cabinets at home, but is instead stored in the cloud on a server. Individuals carry around on their smartphone or tablet all their personal data, shedding light on their relationships, communications and daily contacts. Bodily integrity is no longer limited by a physical barrier because body scanners can breach this integrity from a distance and devices such as sensors and applications that measure body functions can be read remotely.[27]

Privacy (particularly information privacy) and freedom of expression

Privacy and freedom of expression are partly complementary and partly conflicting rights. They are complementary because they protect the thoughts and feelings of the individual expressed in a private setting before they enter the public domain.[28] They are conflicting in cases where secret or private information is divulged in the public interest. The role of the authorities in the former case involves ensuring that people's private acts and opinions are not spied upon and, in the latter case, protecting people's private life and reputation. Undue government interference could also have a chilling effect on people's cognitive development: they might no longer dare to say what they think in their private life.

26 P. Blok, *Het Recht op Privacy* (The right to privacy), The Hague: Boom juridische uitgevers, 2002. B. Roessler, 'New ways of thinking about privacy', in: Anne Phillips, Bonnie Honig and John Dryzek (eds.) *Oxford Handbook of Political Theory*, *Oxford: Oxford University Press, 2006. G. Overkleeft-Verburg, Commentary on article 10 of the Dutch Constitution.* In: E.M.H. Hirsch Ballin and G. Leenknegt (eds.), Artikelsgewijs commentaar op de Grondwet, web edition 2014. See: <http://www.nederlandrechtsstaat.nl>.

27 B.J. Koops, 'On legal boundaries, technologies, and collapsing dimensions of privacy', *Politica e Società,* 3(2), pp. 247-264.

28 See E.J. Dommering and others, *Informatierecht* (Information law), Amsterdam: Otto Cramwinckel, 2000.

Thoughts and feelings which have not been expressed in public may vary from expressions of personal conscience to an exchange of views between a few individuals or within a closed group, without the content of the information or the identity of those concerned being revealed outside the circle. This also includes the processing of information in a private setting, for example borrowing, buying and reading a book, watching a film or listening to an audio source either at home or – anonymously – in a public space (e.g. a cinema or public reading room). Another category is unpublished writings and private data collections. Nowadays, using search engines and consulting and downloading (multimedia) web pages would also be covered. Yet another example of a situation in which a conviction is privately expressed is secret voting in elections and anonymous election results.
In his report of 17 April 2013 to the Human Rights Council, Frank LaRue, the former special rapporteur on the promotion and protection of the right to freedom of opinion and expression, described the connection between freedom of expression and the right to privacy as follows:[29] '*Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a private sphere with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used'* (sic).

LaRue therefore regards privacy and freedom of opinion and expression as being inextricably linked. He writes: '*The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas.*'

Protection of the free and confidential exchange of thoughts and feelings in the private sphere acquired a new dimension with the advent of the postal network. Even thoughts and feelings exchanged over long distances and through the intermediary of a third party (the postal services) were now assured of the same level of protection as if the exchange took place within a defined area (such as a home). This protection of the channel of communication (the privacy of correspondence) therefore also extended to the identity of the sender and receiver. Over time, this protection was extended to other communication channels such as the telegraph and telephone.[30]

Freedom of expression is protected because it plays a critical role in the public determination of the truth, public artistic expression and public democratic decision-making, all of which are core values of an open and democratic society governed by the rule of law. The European Court of Human Rights therefore regards the freedom of expression as the cornerstone of democracy.[31] Anonymity can be a factor here since

29 A/HRC/23/40, sections 22 and 24.

30 See W. Steenbruggen, *Publieke dimensies van privé-communicatie. Een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk* (Public dimensions of private communication. A survey of government responsibility for the protection of confidential communications in the digital age), Amsterdam: Otto Cramwinckel, 2009; E.J. Koops, 'Commentary on article 13 of the Dutch Constitution'. In: E.M.H. Hirsch Ballin and G. Leenknegt (eds.), *Artikelsgewijs commentaar op de Grondwet*, web edition 2014, see: <http://www.nederlandrechtsstaat.nl>.

31 Sunday Times v. United Kingdom, 26 April 1979, Series A, Vol. 30.

people may find it easier to express an opinion freely if their identity is protected. It may also provide a layer of protection in countries where the freedom to express thoughts or feelings in public is not recognised or exercising the right is risky. Protecting the anonymity of whistle-blowers and, in general, of journalistic sources is also a way of helping people to express views freely.

The rights to privacy and freedom of expression can be traced back to the seventeenth century. Privacy initially took the form of freedom of conscience and an inviolable right of private property. Gradually, these concepts came to be redefined by positive law in the constitutions framed in the late eighteenth and early nineteenth century. Privacy of correspondence and the right to frame and express thoughts in private were regarded as the starting point for freedom of expression. Later, the meanings of the rights of privacy and freedom of expression diverged further, because purely personal communications too required protection when posted as letters. The right to privacy of correspondence thus evolved into the right to general protection of the privacy of the postal service and of unopened letters. This right to protection of non-public means of communication continued to co-exist with the general right of privacy, which developed later.

A logical extension of the freedom of expression in the public sphere is the right of access to public information sources, which are essential in forming a considered opinion. In the second half of the twentieth century this prompted a movement in the majority of the Western democracies to enact laws on freedom of information. These laws required government authorities to provide public access to, in principle, all information of importance to the process of government.

Right of privacy and data protection

In the course of the twentieth century the right of privacy became a general right to respect for private life. This is the right to be left in peace by the authorities and others. It therefore acts as a barrier that protects citizens' personal life and that of their immediate family from society and the state. The right is not so much about what kind of information is gathered about individuals (protection of thoughts and feelings) as about the fact that the information is gathered, stored, processed or distributed without their consent. It follows that the gathering of data about individuals is in itself an intrusion because it constitutes interference by the state in private life.

The right of privacy gave rise to a data protection right, which is typically a right that occurs in a welfare bureaucracy and data-driven marketing economy. Just as in the case of communications over a network, the individual forms part of administrative and economic networks with which he may or may not exchange personal data (data traceable to the individual) which is stored, processed and used. Where an authority systematically organises and uses personal data in its possession, it acquires administrative or commercial power over the data subject. This was already the case in the era of paper records, but the volume of recorded data increased rapidly with the advent of the computer and information technology. In the second half of the twentieth century this led to the introduction of separate legislation regulating the gathering, storage and use of personal data. Under this legislation extra restrictions apply to data that qualifies as sensitive. For example, data concerning a person's political opinions and religious or philosophical beliefs as well as other essential aspects of identity such as sexual orientation or health receive greater protection than other personal data. On the other hand, personal data processed by the press also have a special status because not all data protection rules are applicable to them.

The right to data protection has been enshrined as a separate fundamental right in the EU Charter of Fundamental Rights, distinct from respect for private and family life. It is a hybrid right which both protects privacy and regulates the use of information by those in authority.[32] What it has in common with the right of privacy is that it is based on the concept of personal data, in other words information traceable to an individual. Whereas the right of privacy is intended to give individuals control over their private and family life and thus protect it from the outside world, the right to data protection goes further by extending this control to personal data unrelated to private and family life. The aim is to regulate the use of information by the authority (by formulating the purposes for which data may be used and regulating the proportionate collection, processing and use of data) and make it transparent (by ensuring that the individual can consult, check and correct the information).

The right to data protection is growing in importance because the concept of personal data is becoming blurred. Owing to the expanding storage and computational capacity of computers and the increasing electronic registration of the movements and conduct of individuals, it is becoming ever easier to draw up personal profiles based on large quantities of information and use them in the exercise of authority. These data can be collected without the consent of the person concerned and do not necessarily have to be personal data. Profiles not only facilitate the provision of personalised services but they can also threaten privacy because they lead to discrimination and decisions to take action against individuals without corroborating evidence.[33]

The growing practice of collecting data therefore poses an ever greater threat to privacy. In the long run this increasingly undermines the trust of citizens in government and organisations.

Traffic data

Individual communication over networks is possible only if the sender's message reaches the intended recipient. Correct addressing is therefore essential. The address and name of the sender on the envelope are known as traffic data (i.e. data on who is communicating with whom and when), as distinct from the content of the communication. Nowadays, traffic data are also often referred to as metadata. In the case of letters, the traffic data too were often treated as covered by the confidentiality of correspondence in the broadest sense (the postman was therefore entitled to read but not divulge the traffic data) in order to protect the identity of both sender and recipient. The postal services therefore had only a functional relationship with the address, in the sense that they could read it for the purpose of sorting and delivering the letter. The message is separated from the address by the sealed envelope. This also applied to a very large extent to the organisation of the telephone network and telephone exchanges because message and address followed separate circuits.

Whether the privacy of correspondence relates only to the content of the letter or also extends to the traffic data (sometimes referred to as the privacy of post and

32 See Lee A. Bygrave, *Data Protection Law, Approaching its Rationale, Logic and Limits*, The Hague, London, New York, Kluwer Law International, 2002.

33 M. van Otterlo, 'A machine learning perspective on profiling', in: M. Hildebrandt and K. de Vries (eds.), *Privacy, Due Process and the Computational Turn*, London: Routledge, 2013.

telecommunications in the broad sense) has long been a subject of debate in the Dutch literature.[34] The European Court of Human Rights (ECtHR) has included both elements when interpreting the concept of correspondence in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), but has assigned a lower level of protection to traffic data because they do not relate to the content of the communication.[35] This has now been rendered obsolete by advances in electronic communication (see section III.4.1).

III.2 Specific privacy issues

Targeted surveillance, profiling and invisible registration

Fundamental rights are not absolute since they can be limited if they conflict with other rights or interests. Freedom of expression in the public sphere may be limited in the interests of combating unlawful communications such as defamation, racism, terrorism and infringements of privacy. Examples of limiting factors in the case of freedom of expression in the private sphere may be the need to investigate criminal offences or foil attacks that threaten state security or public safety. Fundamental rights may be curbed only if there is a clear and predictable basis in legislation. Moreover, any limitations must be necessary and proportionate in terms of means and duration and must be based on reasonable suspicions about specific dangerous acts, even where the actions of intelligence and security services are concerned.[36]

One of the main risks of profiling based on analysis of metadata obtained by integrated data collection is that decisions to take action against an individual may be based on a constructed profile without corroborating evidence. The system of checks and balances then degenerates into a system of preventive limitation or even elimination of risk factors. What is involved here is not mass surveillance, for example by means of closed circuit television, but targeted surveillance, i.e. identifying and monitoring groups on the basis of certain characteristics. As the emphasis has shifted from interstate wars to fighting terrorism within national borders, the system of specific limitations on individuals has gradually given way to a system of limitations on the freedom of risk groups and categories. In consequence, a person can be stopped and searched solely because he or she fits the profile of an offender, even without being suspected of a specific offence.

Historical traffic data are of major importance in combating crime. A study carried out by the Research and Documentation Centre (WODC) on the Telecommunications Data

34 See E.J. Dommering and others, *Informatierecht* (Information law), Amsterdam: Otto Cramwinckel, 2000, pp. 76 et seq. and A.J.A. van Dorst, 'Het postgeheim' (The privacy of correspondence), in: A.K. Koekkoek, W. Konijnenbelt and F.C.L.M. Crijns, *Grondrechten. Commentaar op Hoofdstuk I van de herziene Grondwet* (Fundamental rights. Commentary on chapter 1 of the revised Constitution). Nijmegen: Ars Aequi, 1982, pp. 279-297.

35 Malone v. United Kingdom, 2 August 1984, Series A, number 82.

36 ECtHR, 1 July 2008, Liberty and others v. United Kingdom, number 58243/00.

(Retention Obligation) Act[37] describes the use made of the traffic data by law enforcement authorities, the Public Prosecution Service and the courts. The study is based on literature research and interviews. Law enforcement authorities make very frequent use of historical data on telephone traffic in relation to a wide range of criminal offences, especially in locating persons and surveying contacts. This can yield exculpatory or incriminating evidence. Judgments, too, regularly refer to such data. As regards internet traffic data, the WODC study notes that the data which have to be kept by law are no longer consistent with current technology and internet use. The Telecommunications Data (Retention Obligation) Act still assumes that internet users log on through a modem, whereas nowadays they are more than likely to use mobile internet or WiFi networks. Moreover, much internet communication is routed through providers which are not based in the Netherlands and therefore not covered by the Dutch legislation.

Law enforcement authorities sometimes use stealth text messages or comparable means to monitor and locate persons. Their use cannot be traced as the messages are not filed. The location information is then used for control purposes. Its existence is denied (a 'known unknown' to use the terminology of former US Secretary of Defense Donald Rumsfeld) or may even be unknown higher up in the hierarchy (an 'unknown unknown' to use the same terminology).

This raises questions about the right of privacy, the right to secret electronic communication and the right to data protection as well as the related legislation.

The role and position of the intelligence and security services

'If we want to preserve the liberties that define us as a democratic society, we must learn to live with risk'.[38]

The problems described above culminate in a discussion about the intelligence and security services, which are dealt with separately here. The Snowden affair has ensured that the debate about the independence and effectiveness of intelligence and security service oversight is once again high on the political agenda worldwide. This is examined in more detail in chapter V.

Intelligence and security services are increasingly using state-of-the-art technology to carry out untargeted data collection. The data are then processed to identify associations with groups (profiles) and individuals. For example, the General Intelligence and Security Service (AIVD) is already intercepting satellite signals as part of the SIGINT (signals intelligence) programme. If in the future the intelligence and security services were to obtain wider powers extending to cable-based communication, this might mean that the cable network and websites could be tapped. This is considered in section V.2.2 below. Under section 28 of the Intelligence and Security Services Act 2002, requests can be made to Dutch telecommunication companies for traffic data relating to their users which these companies are required to retain under the Telecommunications Data (Retention

37 G. Odinot, D. de Jong, R.J. Bokhorst and C.J. de Poot, *De Wet bewaarplicht telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing* (Telecommunications Data (Retention Obligation) Act. The storage and use of data on telephone and internet traffic for investigation purposes), Meppel: Boom Lemma, 2013.

38 David Cole, 'Can the NSA be controlled?', in: *New York Review of Books*, 19 June 2014, p. 17.

Obligation) Act. This Act is based on an EU directive which has since been struck down by the EU Court of Justice.[39]

These bulk data can be shared with friendly intelligence and security agencies abroad. Section 59, subsection 1 of the current Intelligence and Security Services Act merely provides that the Dutch intelligence and security services have a duty to liaise with their foreign counterparts, but does not contain any safeguards regarding proportionality and legal protection in the event of an exchange of data. The Dessens Committee has recommended that the exchange of bulk data with friendly intelligence and security agencies abroad should be regulated by law.[40] At present, the exchange of such data is governed only by administrative rules, which provide that any exchange is dependent on the extent to which foreign agencies comply with criteria such as democratic accountability and respect for human rights. The AIV considers that the legal status of Dutch citizens should be protected by means of safe harbour provisions, limitations on use and access to the courts. In the government's response to the evaluation of the Intelligence and Security Services Act 2002 (i.e. the Dessens Committee's report), the Minister of the Interior and Kingdom Relations writes that the exchange of bulk data with foreign services will be subject to a system of ministerial consent.[41]

The ECtHR has held that the mere collection and storing of personal data amounts to an interference with the right to respect for private life, which may or may not be justified if the requirements of article 8 (2) ECHR have been fulfilled.[42] The bulk collection of apparently innocent data may constitute a breach of the principles of legality, proportionality and effectiveness. As, in practice, the data are often not classified as personal data in the collection stage, the principle of data minimisation in dealings between individuals and the state is becoming less and less significant. It follows that it is now all the more necessary to ensure that the processing, use and dissemination of bulk data are subject to strict standards and oversight. This is the essence of the debate about the intelligence and security services.

Independent oversight of intelligence and security services

One of the main questions that society must answer is how much risk it is prepared to accept in balancing the interests of state security and safeguarding fundamental rights. Theories on cybersecurity distinguish between precluded event security and marginal security cost. The former is an absolute security criterion and is applied to certain vital

39 EU Court of Justice, 8 April 2014, C-293/12 (Digital Rights Ireland Ltd) and C-594/12 (Kärntner Landesregierung); for an explanation of how this affects the Dutch legislation, see Parliamentary Papers, House of Representatives, 2014-2015, 33870, no. 3, See: <https://zoek.officielebekendmakingen.nl/dossier/33870/kst-33870-2?resultIndex=0&sorttype=1&sortorder=4> and the information published by the Advisory Division of the Council of State on 19 November 2014, see: <http://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=287&summary_only=>.

40 Dessens Committee, *Evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen* (Evaluation of the Intelligence and Security Services Act 2002. Striking a new balance between powers and safeguards), December 2013, p. 119.

41 House of Representatives of the States General, 33820, no. 2, p. 7.

42 ECtHR, 4 December 2008, S. and Marper v. the United Kingdom, applications nos. 30562/04 and 30566/04.

systems, such as air traffic control. However, it is unacceptably high for many other systems in society, for example because the financial costs of achieving absolute security are prohibitive.[43] In such cases, the second criterion is applied. The same question must be asked when seeking to strike a balance between the demands of security and the need to enforce rule-of-law values. When it comes to security, it seems that society strives to achieve the unattainable ideal of precluded event security, which can disrupt the proper balance under the rule of law.

Such a tendency to define the concept of security or lack of security in terms of precluded event security and to resort to ever more far-reaching measures in order to exclude all risks could in itself pose a risk to the rule of law, albeit of a very different nature from the terrorist attacks prepared on the internet. It is relevant to ask here how a system of effective and independent oversight should be organised, taking account of the principles of legality and proportionality.

Effective and independent oversight of the covert activities of the intelligence and security services is essential in preserving the rule of law.[44] In the long term this can help to maintain confidence in the rule of law. Various oversight models exist and are often used in combination with one another. The internal scrutiny consists of ministerial oversight and ultimately the accountability of the minister to parliament. A possible drawback of this system is that since the intelligence service is better informed than the minister, he or she may become its captive. At the same time, parliamentary oversight is subject to secrecy, which is hard to reconcile with the usual public nature of parliamentary accountability. External administrative oversight has the advantage that it also covers the question of efficiency of policy measures, but its disadvantage is that it often results in non-binding recommendations. Another important factor is the effectiveness of the oversight. Matters of relevance here are expertise, availability of accessible and complete information, and presentation of the advantages and disadvantages.

In a democracy governed by the rule of law not only must the grounds for limiting fundamental rights be laid down in accessible statutory rules but any limitations imposed by the authorities on the exercise of fundamental rights owing to a pressing public interest must also be subject to effective and independent oversight. The ECtHR,[45] like the Parliamentary Assembly of the Council of Europe,[46] has a marked preference for preventive control by the judiciary. The ECtHR's requirement of judicial control has not been stipulated as an absolute condition in the case of the intelligence and security services, provided that the oversight is otherwise sufficiently independent and effective.

43 M. van Eeten, Johannes M. Bauer, 'Emerging threats to internet security: incentives, externalities and policy implications', *Journal of Contingencies and Crisis Management*, volume 17, issue 4, pp. 221-232.

44 On this subject, see Hans Born and Marina Caprini (eds.), *Democratic Control on Intelligence Services,* Ashgate, Aldershot, 2007, and also: I. Cameron, *National Security and the European Convention on Human Rights*, The Hague: Kluwer Law International, 2000.

45 ECtHR, 29 June 2006, Uzun v. Germany, no. 35623/05, with reference to Klass and Others v. Germany, 6 September 1978, no. 5029/71, § 41 and Malone v. the United Kingdom, 2 August 1984, § 64, Series A, no. 82.

46 Recommendation 1402 (1999)1 of the Parliamentary Assembly of the Council of Europe, *Control of internal security services in Council of Europe member states*.

Preventive judicial control extends beyond individual cases because intelligence and security services also search for unknown risks. In collective cases of this kind, the oversight should focus on whether a specific, targeted programme is the least intrusive option and on the factual underpinning and predictive value of certain profiles. In the course of preventive control, the courts can also scrutinise the duration and modality of a programme.

Preventive judicial control can also compel intelligence and security services to provide better underpinning of both their programmes and their specific activities. Another requirement for critical monitoring of programmes is transparency, for example in the form of publication of statistical data and public reporting.

The Dessens Committee's report discusses in section 4.4 the external oversight of the Dutch intelligence and security services, in particular the oversight by the Intelligence and Security Services Review Committee (CTIVD), parliament and the Netherlands Court of Audit.

In chapter 5 of its report, the Dessens Committee examines in some detail the various forms of preventive oversight applied in a number of countries. It discusses three forms in relation to the use of special powers by intelligence and security services.[47] The first is that in which consent has to be given by the minister responsible (or a civil servant acting on his behalf). This is the variant chosen by the Netherlands and the United Kingdom. Here, decision-making takes place for the most part internally, which is why the ECtHR believes that the exercise of powers is susceptible to abuse. The Dessens Committee therefore considers that these forms of control can function only if they are supplemented by external forms of oversight. A second form of preventive oversight involves the provision of prior advice by an independent committee. This is the variant used in Germany, Belgium and France. In the view of the Dessens Committee, a risk of this variant is that the oversight will be marginal and will tend to focus on procedural aspects. The Dessens Committee believes that adequate powers, a good appointments procedure, proper information and adequate support are essential conditions. Moreover, the independent committee must be permanently available in order to take quick decisions on whether a special power may be exercised. There is also the risk that the authority may show too much understanding for the interests of the intelligence and security services and too little for civil liberty safeguards. The third variant identified by the Dessens Committee is preventive judicial control: a court must grant an authorisation before a special power may be exercised. Countries in which this variant is used include Canada, the United States and Sweden. It is used in the Netherlands only in respect of privacy of correspondence and will also be introduced for inspection of telecommunication data. In most countries, the control is carried out by a single judicial authority so that the information need not be widely disseminated and the judges can specialise.

47 Dessens Committee, *Evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen* (Evaluation of the Intelligence and Security Services Act 2002. Striking a new balance between powers and safeguards), December 2013, pp. 95-100.

The Dessens Committee argues that, in the absence of the relevant data, it is impossible to say with certainty whether preventive judicial control is more effective than other forms of oversight. It notes that a court will not concern itself with whether the exercise of special powers is desirable in policy terms and will instead focus on the legal aspects, for example whether the exercise of the powers is reasonably proportionate to the intended outcome. Ultimately, the Dessens Committee concludes that, broadly speaking, it would be worth introducing an external preventive control on the use of special powers only if it is found that there are no other ways of effectively strengthening oversight in a manner that can be better incorporated into the existing system. All things considered, the Committee ultimately opts for *ex post facto* oversight, provided that this is timely and effective and that legally binding recommendations can be made.

III.3 The internet and freedom of expression: new intermediaries, blurring of distinction between public and private, commercialisation of the public sphere and mobilisation

Hitherto, much attention has been focused on the different aspects of communication in the private sphere, given the emphasis put on this in the request for advice. However, there are also important issues concerning internet communication in the public sphere.

Intermediaries are afforded special protection in the context of traditional forms of communication in the public and private spheres. Messengers too receive preferential treatment: journalists have a right not to divulge their sources because anonymity is seen as a way of promoting public debate. The public broadcasting organisations were seen as a means of promoting pluralism and facilitating access for minorities. A broad cultural policy guaranteed the maintenance and accessibility of important sources of information such as public and university libraries. Publishing houses share in these privileges. Over the centuries all these intermediaries have been exempted from substantive government interference in Western countries.

The internet has spawned a new family of important intermediaries, who are partly replacing the old intermediaries. The protection for the role of these intermediaries has not yet been formalised in legislation. Where access to the network (the typical telecommunication function) is concerned, there are rules in the United States and the EU which provide for equal access for service providers and users. This is known as the principle of network neutrality. The internet service providers which convey the information to and from the user enjoy limited protection in the EU under the caching and hosting safe harbour provisions of the EU's Electronic Commerce Directive.[48] They benefit from these electronic communication rules because they cannot be held liable for the (illegal) content of information which they store briefly or retain for longer in the course of the transmission in order to facilitate requests by the user, provided that they remove manifestly illegal content as soon as they receive notice from an interested party (the notice and take-down procedure). The position of intermediaries which generate and pass on facts and opinions, such as websites, is much less clear as they fall between media and telecommunication rules. The position of important intermediaries like search engines is still the least clear. While they are distributors and users of personal data on a massive scale, they are also increasingly an essential link in the global network for the provision of access to information sources. This is why they should have their own

48 Directive 2000/31/EC.

status under the rules on freedom of expression, but this is still a long way off.[49] The same is true of all intermediaries (e.g. specialised search engines, Wikipedia and so forth) which focus on systematically classifying and providing access to information, for example by means of hyperlinks.

In the case of media communications in the public sphere and individual communications on social media it is becoming increasingly difficult to identify who is responsible for a particular communication, owing to the intricacy and, for the average user, unclear organisational structure of the internet. This is bringing about a shift towards collective responsibility of the intermediaries, in that there is a growing tendency to hold them liable for socially undesirable information distributed through their platform, regardless of whether or not they have anything to do with it.

Another related development is the emergence of a new type of intermediary, namely the social media organiser, which hovers somewhere between the public and private spheres. Examples are Facebook and YouTube. Here too, it is still unclear whether they are governed by telecommunication or media rules. So it seems that offline cannot be translated one-on-one into online, which requires its own solutions.

These new and powerful commercial intermediaries have been taking over more and more public media functions, at the expense of pluralism. The design of the public space and the public debate has thus become increasingly privatised. The public sphere is determined not by the public interest that underlies the actions of public media institutions but by commercially driven information paths marked out by the new media.

Traditionally, the mass media have also had a mobilising function. This has now been strengthened and given many new dimensions by the advent of the internet and the social media. Every new advance in communication technology is employed for emancipatory purposes. At the time of the fall of the Berlin Wall that was the fax machine. Later the same function was fulfilled by the mobile phone and email. The street protests and demonstrations in Europe (Occupy) and later in Turkey and the Middle East have been driven by social media such as Twitter and Facebook. Often they have been backed by traditional media outlets such as the Guardian and Al Jazeera, which have skilfully capitalised on these events. This new dimension is also visible in the revelations of Assange and Snowden.

III.4 The relationship between legal concepts, technology and sovereignty

The internet (together with the related ICT) confronts us with two essential questions. First, whether legal concepts and the related notions of protection still reflect the underlying reality, which has changed constantly as a result of market forces and advances in information technology. Second, what significance the sovereign nation-state has in borderless cyberspace.

49 J. van Hoboken, *Search Engine Freedom, On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*, Alphen aan den Rijn: Wolters Kluwer Law & Business, 2012 (Information Law Series no. 27). See also the analysis of the Google judgment in section V.3.1.

III.4.1 Law and technology: privacy of communication, traffic data, security and intermediaries

Scope of privacy of communication

These questions lie at the root of the Dutch struggles with the concept of privacy of communication. The Dutch government submitted a proposal to amend article 13 of the Constitution (privacy of correspondence and privacy of the telephone and telegraph) to the House of Representatives on 16 July 2014.[50] The argument on which this proposal is based is that the provision needs to be modernised as a matter of urgency in order to ensure that protection also extends to email in the future. The term 'privacy of the telephone and telegraph' is to be replaced by the more generic term 'privacy of telecommunication', which differs from the term 'electronic communication' used by the EU. Equating privacy of correspondence with privacy of telecommunication means, however, that the high level of protection afforded to traditional correspondence will disappear. Hitherto, the intelligence and security services have not been able to open letters without prior judicial authorisation. Although the scope of the protection in the Constitution is to be broadened, its level is to be lowered. This means that the legislator has chosen to scrap the legal protection guarantees in the Constitution and that rules on the proportionality of any limitation of the rights will in future be contained solely in ordinary legislation.

A related matter which gives rise to recurrent discussion in the context of the confidentiality of telecommunication is whether unencrypted and unaddressed signals are entitled to the same level of protection as communications over a clearly defined channel. The reasoning is that signals available everywhere on the airwaves (i.e. signals capable of being received by everyone) are not entitled to the same level of protection because there is no reasonable expectation of privacy when this medium is used. This concept has been developed by the US Supreme Court, but is a matter of growing debate in the United States. This is why the Dutch Intelligence and Security Services Act 2002 provides for a lower level of protection for unaddressed signals. This is a legacy of the controversy about the Echelon Project – a collection and analysis network jointly operated by the intelligence and security services of English-speaking countries – which led to a public debate in Europe at the start of the century.[51] The Dutch legislator has also introduced stricter rules for the interception of cable transmissions, which may be tapped only if the sender is known. The Dessens Committee has proposed that this distinction should be abandoned. Such an amendment is likely to have the same effect as in the case of privacy of correspondence: the threshold for tapping the communication infrastructure will be lowered. This matter is discussed in more detail in section V.2.2.

In both cases, the scope of protection has therefore been widened and the level of protection lowered. Three examples may show that advances in technology necessitate revision of the constitutional and statutory provisions.

50 House of Representatives of the States General, 33 989, nos. 1 and 2.

51 European Parliament, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), 11 July 2001.

Traffic data

The first example relates to the status of traffic data, which has already been dealt with in relation to privacy of correspondence in section III.1. The ECtHR's 1984 judgment (see section III.1) has been rendered obsolete by the fact that traffic data are not content-neutral and can actually shed much light on the nature of the contacts and the context (and hence the content) of communications sent and received, particularly when combined with information about, say, the internet browsing behaviour of the sender and recipient of the message. As a result of technological advances, the traffic data have gradually yielded more and more information about the senders and recipients of messages. Originally they said something about when and how often a data subject sought contact with certain persons. Other traffic data added in the mobile phone age were the location of sender and recipient, because mobile phones – when turned on – are in continuous contact with a dense network of transmitter masts, each of which has its own specific reception area. In the internet age the volume of traffic data has grown exponentially and these data are now also stored temporarily. And here the statistical Big Data rule applies: the greater the volume of data, the more light they shed on the personal preferences of the person concerned and the nature of his or her activities and individual contacts. The distinction between addressing and content is further blurred in the case of internet communications by the fact that the two overlap seamlessly, without any clear protective barrier (like a sealed envelope in the case of postal correspondence) between them. Traffic data provide an intrusive glimpse into a person's private life, even if they provide little or no insight into the content of the communication.[52] In addition to traffic data leaving traces on the internet from which personal data can be gleaned, the Internet of Things will lead to an increase in the volume of digital data shedding light on the way of life and preferences of internet users. And numerous other metadata can provide revealing information as well.

This raises the question of whether such data should be legally protected and, if so, how. The bill to amend the Constitution does not deal with this problem, leaving it to the legislator to define this fundamental right. No matter how traffic data are defined, there is no reason to allocate them a relatively low level of protection.

Processing and security of personal data

The second example relates to the arrangements for the processing and security of personal data. The data protection provisions are based on the central concept of processing. It has been noted above that the concept of personal data is giving rise to ever more problems since in the age of Big Data the individual only comes into the picture when the damage has already been done. A similar problem occurs in relation to the broad definition of processing and the related duty of security. The usual legal definition of processing covers operations of unlike nature in technical terms, for example collection, storage and dissemination, together with all other intermediate computer operations. Providers of cloud services are obliged to ensure adequate security for their services to prevent hackers from gaining access to the data. Government bodies may request data from the cloud and compel the service provider to decrypt the data. Users

52 B.J. Koops and J.M. Smits, *Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie* (Traffic data and article 13 of the Constitution. A technical and legal analysis of the difference between traffic data and the content of communication), Wolf Legal Publishers, 2014.

can combat this only if they themselves encrypt all data themselves before sending them to the cloud. However, few users do this because they rely on the security provided by the service provider and also because storing encrypted information in the cloud is inefficient for various applications. As computers find it hard to compute using encrypted data, the computing capacity of the cloud can no longer be used.[53]

The gaps in the duty of security are of real importance because crucial interests are at stake. The cloud is organised for the most part by US companies and there is a real likelihood that information entrusted to the cloud by Dutch individuals and institutions will end up subject to US jurisdiction. This means that the data will become accessible to the US authorities.[54] It should be noted here that since the Snowden revelations it has been uncertain whether the intelligence and security services have inserted backdoors into encryption technology. This means that users are in danger of losing control of their data. During the German occupation of the Netherlands in the Second World War, the resistance movement attacked the Amsterdam population registry in an effort to frustrate the efforts of the Germans to prosecute and deport members of Amsterdam's Jewish community. This attack is sometimes cited in the Netherlands as an early example of how civil liberties were protected against the risks posed by data storage in public registers. In 2014, however, such an act would serve little purpose because, through the cloud, the data would probably already be accessible to a foreign power outside the territory of the Netherlands.

Transport and content

The third example relates to the concepts of media law (responsibility for content) and communication and telecommunication law (no responsibility for content). In the Netherlands it used to be said that 'the PTT reads the envelope, not the message'. However, the technical reality is more complex because it is increasingly based on the automatic classification and indexing of the content of messages, without the operator having editorial responsibility for content. The search engine does more than transport but less than edit the message. Its role more closely resembles that of a library. A law which fails to recognise this new intermediary function, which is positioned somewhere between transport and editing, imposes responsibilities where they do not belong and may thus jeopardise the critical role now played by the search engine in the information provision process.[55]

These examples show that the relationship between the values requiring protection need to be aligned with the technical processes.

III.4.2 National sovereignty: jurisdiction and fundamental right violations

The internet is increasingly laying bare an old conflict in public international law, namely that between the concept of the universal world community of citizens on the one hand

53 C. Bowden, *The US surveillance programmes and their impact on EU citizens' fundamental rights*. Note, European Parliament, 2013, p. 33.

54 This issue was raised for the first time in the Netherlands in 2013 by J. van Hoboken, A. Arnbak and N. van Eijk, in: *Obscured by the clouds*. See: <http://www.ivir.nl/publications/vanhoboken/ obscured_by_clouds.pdf>.

55 See also III.3.

and the protection by a nation-state of its own citizens (to the exclusion of other citizens) subject to its power monopoly on the other. Although the structure of the internet exhibits post-Westphalian era traits, the Snowden affair has revealed that the conflict is actually more than ever between national and regional legal communities.[56]

The production, dissemination and storage of information on the internet is no longer bound by place and time. The commercial organisations are using global networks in which decisions on where data are produced and stored are made on economic grounds. The cloud is an example. Government organisations (such as intelligence and security services) are entering into forms of cross-border cooperation in which they share information with one another. Personal data databases in different countries are increasingly interlinked. As web pages can be accessed worldwide, the scope of public media communications now extends far beyond the national domain for which they were originally intended. Moreover, internationally oriented electronic internet media are also now in existence.

In general, the national private service providers operate within a clearly defined national or regional jurisdiction. After all, the offices, physical infrastructure and support services and equipment which connect the user with the internet are located in one or more specific jurisdictions. This determines what rules apply to access, security and use for a given user. As global players such as Google operate in many national markets, it is not always clear under which legal system they fall. All of this leads to conflict between different national and regional legal and policy regimes of fundamental rights, which have not yet been resolved. Unlike the European Convention on Human Rights, US constitutional law is based on protection of persons having US citizenship (*we, the people*) and US residents. As many important intermediaries are American and fall under US federal law, it follows that information entrusted to them in the cloud by non-American citizens who are also not US residents is not entitled to protection under US law. In the United States, discussion about the Snowden affair is therefore largely confined to the fact that American citizens were tapped and electronically monitored by the National Security Agency (NSA). It is necessary to wait and see how this will be dealt with in the judgments of the EU Court of Justice and the ECtHR. US law is explained in more detail in section V.2.1 below.

The questions which arise here are whether citizens of a different nationality enjoy the same protection in other jurisdictions as they do in their own country or region, to what extent national authorities must take measures to ensure the national or regional level of protection even outside their own jurisdiction, to what extent they can impose obligations on private service providers for this purpose and how service providers can or should deal with conflicting or possibly irreconcilable demands from different jurisdictions in respect of certain groups of customers. One of the measures which European governments could take to protect their vital interests (as Chancellor Merkel has already proposed) is to make it possible for certain information to be sent exclusively through European infrastructure and for data not to be stored in a cloud which is physically or legally outside European jurisdiction. These are interesting options, but probably unrealistic. Safe harbour agreements cannot guarantee the same level of protection for the reasons mentioned here and in the previous section. This is also why the imposition of obligations on companies for activities that take place outside the EU is problematic.

56 A. Linklater, *The Transformation of Political Community. Ethical Foundations of the Post-Westphalian Era*, Oxford: Polity Press, 1998.

IV The main legal frameworks

The fundamental rights discussed above are enshrined in international and regional conventions, constitutions and other national primary and secondary legislation. At global level the instruments and bodies concerned are UN conventions and organisations. At European level they are the conventions and constituent organs of the Council of Europe and the EU. All EU member states are also members of the Council of Europe, but the latter has many more members (including Russia and Turkey). An organisation which makes effective use of non-legal instruments to shape policy in relation to the internet in Europe is the Organisation for Security and Cooperation in Europe (OSCE), but this is beyond the scope of this report.[57]

IV.1 The UN

The Universal Declaration of Human Rights and the resolutions of the UN General Assembly and the Human Rights Council contain universally shared standards and values. The main global convention relating to internet freedom is the International Covenant on Civil and Political Rights. This plays a less prominent role in Europe because the rights and freedoms it contains are also included in the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights, both of which have stronger enforcement mechanisms.

In July 2012 the Human Rights Council adopted a resolution on the promotion, protection and enjoyment of human rights on the internet (A/HRC/20/L.13), which emphasised freedom of expression. The resolution affirms that people have the same rights online as offline, calls on states to promote and facilitate access to the internet and requests the special rapporteurs to take these issues into account within their existing mandates.

The Snowden affair has pushed privacy and the internet higher up the UN's agenda as well. On 18 December 2013 the UN General Assembly unanimously adopted resolution 68/167 (The right to privacy in the digital age),[58] which had been proposed by Brazil and Germany. The resolution affirms that offline rights also apply online, in particular privacy. The resolution calls upon states to ensure that their national legislation is in compliance with their international obligations, to put an end to violations of rights and to strengthen oversight of intelligence services. The UN High Commissioner for Human Rights is also requested to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data to the General Assembly at its 69th session (September to December 2014). In late June 2014 the UN High Commissioner for Human Rights published a report setting out international law on the promotion and protection of the right to privacy. The report has generated much interest, especially within the internet community, since it reveals that many countries fail to comply with the proportionality principles developed in it. Section 47 of the report concludes that international human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and

57 See: <http://www.osce.org/what/media-freedom>.

58 A/C.3/68/L.45.

extraterritorial surveillance, the interception of digital communication and the collection of personal data. Practices in many states have, however, revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy.[59]

Chapter II of this advisory report has briefly described what internet-related activities are undertaken by the UN organisations. Although the ITU's role is diminishing in significance, the IGF has an important to play in internet governance and must continue to evolve.

IV.2 The Council of Europe

IV.2.1 The Committee of Ministers and the Parliamentary Assembly

Both the Committee of Ministers and the Parliamentary Assembly of the Council of Europe have adopted various declarations and recommendations on internet freedom.[60] In general, they have endorsed ICT's contribution to freedom of expression and the freedom to have access to information, and have also pointed to the drawbacks, namely that ICT can also be used for censorship. It should also be noted that the rights to freedom of expression, information and communication apply independently of the chosen medium. It makes no difference whether these rights are exercised on digital or other media. The Committee and the Assembly have also adopted declarations and recommendations concerning openness and accessibility and the use of internet filters. Naturally, these political declarations and recommendations are important, particularly if they are reflected in conventions and legislation. However, it would be beyond the AIV's remit to consider each separate declaration or recommendation.

IV.2.2 The European Court of Human Rights

The European Court of Human Rights (ECtHR) gives judgments on the interpretation of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) which are binding on the member states of the Council of Europe. Some cases of special relevance to internet freedom are discussed below.

Article 10 ECHR

The ECtHR has interpreted articles 8 and 10 ECHR in the light of changing technologies and the demands of the time. In doing so, it takes account of the resolutions and declarations of the Parliamentary Assembly and Committee of Ministers. These judgments provide guidance when the EU Charter of Fundamental Rights is interpreted. The ECtHR has repeatedly commented on the essential role played by the press (including the electronic mass media) in relation to democracy. Some of the most noteworthy judgments are considered below.

59 Report of the Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/27/37, 30 June 2014.

60 For example, the Declaration of the Committee of Ministers on Human Rights and the Rule of Law in the Information Society (CM(2005)56 final of 13 May 2005), Recommendation CM/Rec(2007)16, Recommendation CM/Rec(2007)11, Recommendation CM/Rec(2008)6 and Recommendation CM/Rec(2012)3.

The first is the Yildirim case (ECtHR, 18 December 2012, appl. no. 3111/10). On 23 June 2009, under section 8 (1) (b) of Turkish Law no. 5651, which regulates internet publications and is intended to combat internet offences, the Turkish Denizli Criminal Court of First Instance ordered the blocking of a website on which publications insulting the memory of Atatürk had been posted. This site was hosted by sites.Google.com. The order was made in the context of proceedings against the owner/operator of the website. The Turkish Telecommunications Directorate, which was tasked with executing the order, then proceeded to block access in Turkey to sites.Google.com, as this was thought to be the only effective way of blocking access to the offending site. However, this meant that access to all other sites on sites.Google.com was also blocked in Turkey, including that of Mr Yildirim. The Turkish judges held that this was the logical and hence acceptable consequence of the object of the original order, i.e. preventing further online insults to Atatürk's memory.

The ECtHR held that since the blocking meant that no one could gain access to Yildirim's website (not even himself) it was contrary to article 10 of the ECHR. In its judgment the ECtHR referred to all relevant European and UN declarations and resolutions on internet freedom. Although the guiding principle that can be inferred from them is that prior restraint is not permitted, the ECtHR stuck to its view that the Convention does not contain an absolute ban on censorship. Paragraph 64 of the judgment reads as follows: 'The Court considers that such prior constraints are not necessarily incompatible with the Convention as a matter of principle. However, a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power.'

The applicant in these proceedings, who could no longer gain access to his website as a consequence of this measure, succeeded in his action. This means that the ECtHR has brought free access to the internet within the protection of article 10. Of particular importance to internet freedom is paragraph 67, in which the ECtHR holds that the blocking order was in direct conflict with article 10, paragraph 1 of the Convention, which expressly provides that the rights are secured 'regardless of frontiers'. The ECtHR refers in this connection to paragraph 62 of the Ekin case[61] in which it had condemned the banning of foreign publications. That means that the place where access to the World Wide Web is effectively blocked and not the place of establishment of the hosting service is relevant. If the place where it is blocked is in a state which is a member of the Council of Europe, the Convention is applicable. Conversely, a resident of another country cannot complain about communications in a country that is a member of the Council of Europe to which he has access through the internet.[62] In its judgment of 11 December 2006 in the case of Ben El Mahi v. Denmark (appl. no. 5853/06) concerning a complaint by a Moroccan national against Denmark, the ECtHR held that the complaint was inadmissible because Denmark had no jurisdiction over the applicant. This judgment concerned the publication in Denmark of cartoons depicting the prophet Muhammad. What happens if the consequences of violations of fundamental rights committed in a country that is not a member of the Council of Europe have a knock-on effect in areas over which the Council

61 Note by E.J. Dommering on Association Ekin v. France, ECtHR, appl. no. 39288/98, 17 July 2001, in: NJ 2002, 444.

62 N. Vajic and P. Voyatzis, 'The internet and freedom of expression and the ECHR's evolving case-law', in: Joseph Casadevall and others (eds.), *Freedom of Expression*, Oisterwijk: Wolf Legal Publishers, 2013, p. 403.

of Europe does have jurisdiction is still undecided. This question has become extremely topical as a result of the Snowden affair.

Where citizens of a country that is a member of the Council of Europe consider that their rights as guaranteed by the Convention have been violated on the internet, they may therefore invoke the provisions protecting their rights before the national and European courts. However even if these courts hold that they have jurisdiction and that there has been a violation, this does mean that such a decision will be recognised in a country that is not a member of the Council of Europe, for example the United States.

On 6 July 2014 the Grand Chamber held a hearing in the case of Delphi v. Estonia (appl. no. 64569/09), which concerned the liability of an internet service provider for the content of information posted on the internet. In due course, the ECtHR may give a more general ruling in this case on the internet's role in a democracy.

Article 8 ECHR

The ECtHR has developed the procedural safeguards of data protection law on the basis of article 8 ECHR (right to respect for private and family life) by interpreting this provision as creating a positive treaty obligation to create national safeguards against violation.[63] It was noted in section III.1 above that the ECtHR had brought traffic data within the scope of article 8.[64] Later it did the same with email.[65] The ECtHR also states very explicitly that the mere collection of data constitutes an interference with privacy.[66]

In the context of mass surveillance the ECtHR's decision in the Liberty case is becoming increasingly relevant.[67] This case concerns the actions of the British Ministry of Defence in the 1990s, when it started intercepting all telecommunications between Dublin and London. The main part of the complaint was that the telephone calls were filtered using secret filtering criteria, although a proper warrant had not been issued. The complaint was upheld by the ECtHR. The interception process involves five stages. First, a warrant would be issued specifying the communication links to be intercepted.

63 Gaskin v. the United Kingdom, ECtHR, 7 July 1989, Series A, appl. no. 160, NJ 1991, 659 with note by E.J Dommering. 1981 saw the entry into force of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which regulates the general principles of the automatic processing of personal data, namely that collection, storage, processing, use and dissemination may take place only with consent for the purpose concerned or for a justified purpose and must be proportionate (no more and no longer than necessary for the purpose for which they have been collected), correct and transparent (right of inspection and correction). This convention has served as a model for many national laws in Council of Europe countries and the directives drawn up later by the EU.

64 Malone v. the United Kingdom, ECtHR, 2 August 1984, Series A, appl. no. 82, see also NJ 1988, 534 with note by E.J. Dommering.

65 Copland v. the United Kingdom, ECtHR, 3 April 2007, appl. no 62617/00; see also NJ 2007, 617 with note by E.J. Dommering.

66 S. and Marper v. the United Kingdom, ECtHR, 4 December 2008, appl. nos. 30562/04 and 30566/04.

67 Liberty and others v. the United Kingdom, ECtHR, 1 July 2008, appl. no. 58243/00. NJ 2010, 324, with note by E.J. Dommering.

Such warrants covered very broad classes of communication, for example all commercial submarine cables having a terminal in the UK. Next, the Secretary of State would issue a certificate describing the categories of information which could be extracted from the total volume of communications intercepted under the warrant. The next stage involved the installation of filter systems. These were automated search engines which selected communications containing specific search terms or combinations thereof. The following step was to clean up the filtered communications by removing names or details which were not necessary for the purposes of the interception.

As usual in cases of this kind, the ECtHR considered at some length whether the statutory provisions and the criteria by reference to which the right is exercised are sufficiently accessible and foreseeable to be in accordance with the law. These criteria had been summarised by the ECtHR in paragraphs 93-95 of its admissibility decision in the case of Weber and Saravia v. Germany, 29 June 2006, appl. no. 54934/00, which also involved the interception of communications in accordance with a system of catchwords.[68] These criteria were quoted in full in paragraph 62 of the Liberty case. The ECtHR has developed the criteria on the basis of individual communication interceptions. They form a five-stage test, which takes the following form:

1. Is there a definition of the categories of people liable to have their communication intercepted?
2. Is there a limit on the duration of the interception of communications?
3. Is there a procedure to be followed for examining, using and storing the data obtained?
4. Are there precautions to be taken when communicating the data to other parties?
5. In what circumstances may or must the data be destroyed?

These are general rules which the ECtHR has formulated for interceptions of electronic communications, which cannot therefore be automatically applied to every situation. The situations may vary from the monitoring and recording of a person's image by electronic means (security cameras in the cell)[69] to the recording of data on a person's way of life and statements in the registers of the intelligence and security services[70] and the monitoring and recording of a person's (electronic) communication activities (both the content and where and with whom).[71]

The ECtHR held in the Liberty case that the five-stage test also applied to strategic monitoring: 'The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.'

68 These rules can also be found in the earlier Huvig and Kruslin judgments, but were then focused on individual forms of monitoring. See also NJ 1991, 523, with note by E.J. Dommering.

69 Perry v. the United Kingdom, ECtHR, appl. no. 63737/00, 17 July 2003. See also NJ 2006, 40, with note by E.J. Dommering.

70 Segerstedt-Wiberg and others v. Sweden, ECtHR, appl. no. 62332/00, 6 June 2006. See also NJ 2009, 449, with note by E.J. Dommering.

71 Copland v. the United Kingdom, 3 April 2007, ECtHR, appl. no. 62617/00. See also NJ 2007, 617, with note by E.J. Dommering.

In September 2013 various human rights organisations applied directly to the ECtHR in proceedings against the United Kingdom. The question they have put to the ECtHR is whether, in the context of its cooperation with the US National Security Agency (NSA), the British intelligence services have acted lawfully in intercepting transatlantic telecommunications on a large scale for the NSA (or arranging for the NSA to intercept them).[72] It remains to be seen in this case whether the ECtHR will tighten up its five-stage test by requiring substantive proof of the need for the programme.

IV.3 The European Union

IV.3.1 General

The EU has developed internet freedom norms based on the free movement of goods and services as enshrined in the European legal order, the acquis communautaire of the constitutional standards and values common to the national legal systems and, after its adoption and ratification, the Charter of Fundamental Rights of the European Union. These norms are intended to harmonise the national legislation of the EU member states. Pursuant to article 53 of the Charter, the EU Court of Justice takes account of legal developments relating to the ECHR when interpreting these norms. In brief, harmonisation in relation to the freedom of expression is defective and fragmented. And this is even more true of technology and privacy.

Electronic communication

The first measures to harmonise communication technology were focused solely on voice telephony (the Open Network Provision / ONP). Gradually, the scope of these measures was extended to full harmonisation of a package of rules covering electronic communication and communication services, but not content-related services.[73] Ultimately this package will have to be implemented in a regulation.[74] Two privacy directives have been adopted: the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data[75] and the Directive on privacy and electronic communications.[76] Subsequently, an exception was made to the latter directive when it was provided that traffic data connected with public order and security could be retained for longer. This was because they needed to be stored for longer than warranted by the purpose criterion. This was recorded in the Data Retention Directive. However, as this directive was declared invalid by the EU Court of Justice in April 2014, the data retention laws based on it must be recast.[77] A framework decision providing specific data protection rules in the area of police and judicial cooperation in criminal matters was adopted under what was then the Third Pillar. The general data protection rules of this

72 Big Brother Watch and others v. the United Kingdom, ECtHR, appl. no. 58170/13, see: <http://www.echr.coe.int/Documents/CLIN_2014_01_170_ENG.pdf>.

73 Recital 5 of Framework Directive 2002/21/EC.

74 COM/2013/0627 final - 2013/0309 (COD).

75 Directive 95/46/EC, 24 October 1995.

76 Directive 2002/58/EC, 12 July 2002.

77 Directive 2006/24/EC, 15 March 2006.

package must be harmonised in a regulation. The framework decision must be replaced by a directive.[78] This set of rules has implications for internet freedom.

The Charter of Fundamental Rights of the European Union has opened a new chapter in this process since it requires the EU Court of Justice to assess the application of primary and secondary EU law in the light of the fundamental rights contained in it. The Charter must also be observed by member states in fields that come within the scope of EU law. A good example is the decision in the case of Scarlet v. SABAM,[79] where the Court of Justice held that the exercise of the right to impose an injunction should be based on the Directive on copyright in the information society.[80] In paragraph 45 the Court of Justice holds that 'in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures'. This reasoning, which has a significant bearing on the free accessibility of the internet, had previously been employed when EU citizens lobbied to reject the Anti-Counterfeiting Trade Agreement, which would have given rights holders far-reaching powers to deny internet access to the users of illegal content.

Freedom of expression

The legislation in this field is fragmented because the EU has to contend with a broadcasting industry whose organisation is very deeply rooted in national traditions. This is why the Audiovisual Media Services Directive does not get beyond coordinating a number of rules relating to advertising.[81] At the time of the most recent amendment, the EU attempted to respond to internet-related developments by introducing a pair of new concepts to complement the traditional concept of the broadcasting media. These new concepts are linear media services (mass communication in the traditional sense) and non-linear media services (a central audiovisual service that provides an interactive service for the user). This is an example of a legal term that bears no relation to the underlying information technology, of which some other examples were given in section III.4.1 above.

Also important is the E-Commerce Directive, which applies to the area not covered by the communication directives and the Audiovisual Media Services Directive. It contains a number of provisions which indemnify intermediary service providers against liability for transmitting content either in the case of mere conduit or in the case of caching and hosting. The terms used in this directive were mentioned in section III.4.1 as an example of legal concepts which are not sufficiently in tune with the underlying technical reality. The parts of this directive of most relevance to this advisory report are the provisions prohibiting prior authorisation for access to services and prohibiting generic monitoring of users of services.[82]

78 COM (2012)10 and COM (2012)11, both of 25 January 2012.

79 Case C-70/10, CJEU, 24 November 2011, with note by E.J. Dommering, in: AMI 2012-2, pp. 49-53.

80 Directive 2002/29/EG.

81 The Audiovisual Media Services Directive 2010/13/EU.

82 Case C-360/10, CJEU, 16 February 2012 (Sabam v. Netlog).

Legislation can have unintended effects if rules are applied in an area for which they were not designed. This is another aspect of the concept of processing discussed in section III.4.1 in connection with the cloud. The EU Court of Justice has applied the concept of personal data processing to the editing of webpages (it had little option given the broad definition employed by the legislator). This occurred relatively early on (in the Lindqvist judgment in 2003).[83] As a result, a system and set of terms originally designed for databases have also become applicable to virtually all web publications (since they almost always involve some personal data processing).

IV.3.2 The EU and privacy

The normative framework of the privacy rules has led to a number of issues, which will be considered briefly below. These are the adoption of the Data Protection Regulation, the negotiations with the United States following the Snowden affair, and the application of fundamental rights criteria by the EU Court of Justice.

The Data Protection Regulation

The major differences that currently exist between the EU member states in the implementation of the privacy directives are encouraging organisations to base their operations in countries where the system is most favourable for them. The purpose of adopting a regulation is to introduce a fully harmonised framework for the entire EU, thereby precluding forum shopping. As the proposed regulation is based largely on the existing set of terms, the defects previously noted will continue to exist. On the other hand, the rules are being tightened up in numerous areas (for example, in relation to profiling, the use of cookies and so forth). One point which remains controversial is whether the system of oversight should be European or should be national and coordinated at European level (as in the electronic communications sector). The US approach becomes relevant here because the proposed regulation relies very heavily on a self-regulation model (described as 'binding corporate rules') in relation to the exchange of data with non-EU countries. Often these exchanges will involve US companies which are subject to US jurisdiction and collaborate, voluntarily or otherwise, with the NSA. What remains to be resolved in connection with the exchange of data with third countries is how a good balance can be struck between adequate legal protection and the smooth exchange of data in a global economy.

Relations with the US

The privacy legislation in the United States distinguishes between the private and public sectors. The private sector is regulated in the United States by the Federal Trade Commission (FTC). The FTC enforces compliance with principles which do not differ greatly from their European equivalents. However, the sanctions that can be imposed by the FTC are often higher than those available to the data protection authorities in Europe.

Under the European Data Protection Directive currently in force, member states are obliged to prohibit the transfer of personal data to third countries which do not provide adequate data protection. To enable personal data to be transferred to the United States under the directive, the Safe Harbour Framework has been agreed. This provides US

83 Case C-101/01, CJEU, 6 November 2003, Jur 2003, p. 1-2971. This was preceded by other decisions, for example the Promusicae judgment of 28 January 2008 (C-275/06, Jur 2008-I-271), in which the Court of Justice held that protection of an intellectual property right had to be balanced against other rights.

companies with the possibility of registering as an entity providing an adequate level of protection. The procedure involves self-certification: the companies themselves are obliged to declare that they will comply with the seven Safe Harbour principles. If desired, they can call in external experts to give an independent opinion. The companies must register each year with the Department of Commerce, which keeps a list of certified companies.

Following the report of MEP Claude Moraes on the Snowden affair in early 2014,[84] the Commission was pressured to terminate the agreement. According to the report, the Safe Harbour Agreement provides insufficient protection for European citizens and is not adequately complied with. Moreover, the definitions of the exceptions relating to national security are too broad in the agreement. There is still no consensus about possible termination of the agreement. The system of oversight was always weak because it relates only to part of the transferred data and is largely based on self-certification by companies.[85] The decision on continuation or alteration of the Safe Harbour Agreement is a matter for the European Commission. The Netherlands supports the position taken by the European Commission, namely that parts of the agreement must be renegotiated and that termination of the agreement would worsen the position of the private sector.[86] However, the Netherlands has more than sufficient expertise to play a more leading role in these discussions.

As regards the transatlantic exchange of data in the public sector, there is at least one example of specific agreements in this field, namely the EU-US Agreement on SWIFT bank data transfer (the Terrorist Finance Tracking Programme – the TFTP Agreement). The European Parliament is demanding suspension of this agreement on the grounds that the Snowden revelations have shown that it has been violated, although this has been denied by the European Commission. However, the agreement clearly has major shortcomings: the protections provided for in relation to privacy and access to and correction of individual data have proved in practice to be virtually unenforceable. According to the first report of the EU-US commission which oversees compliance with the agreement, individual requests for access to and correction of personal data cannot be granted. This is either because the data in question cannot be retrieved from the larger data set since the authorities in the United States may only request data connected with terrorism or its financing or because the data are dealt with in the context of confidential terrorism-related investigations about which no disclosures may be made. In practice, therefore,

84 Draft report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Committee on Civil Liberties, Justice and Home Affairs, rapporteur: Claude Moraes, 2013/2188 (INI).

85 C. Connolly, *EU/US Safe Harbour, Effectiveness of the Framework in relation to National Security Surveillance,* Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on electronic mass surveillance of EU citizens, Strasbourg, 7 October 2013.

86 House of Representatives of the States General, 32 317, no. 226, pp. 12 and 13.

the legal protections in the TFTP Agreement have proved inadequate.[87]

Negotiations are now under way between the EU and the United States to prepare an umbrella agreement for the public sector. One of the difficulties is that the Charter of Fundamental Rights of the European Union requires control by an independent data authority – a concept which is unknown in the United States. Another stumbling block is the fundamental gap in public international law between a sovereign state which protects only its own citizens and the universality principle, which confers the same rights on people throughout the world. The US government does not wish to give European citizens a legal remedy before the US courts (see section III.4.2). Although there are no major differences of opinion about what constitutes privacy protection, there are disagreements about what exceptions should be allowed in the interests of national security, which is defined much more broadly by the United States.

Application of fundamental rights criteria

In this field too, the effect of the Charter of Fundamental Rights of the European Union has quickly become apparent. The EU Court of Justice declared the Data Retention Directive to be invalid because it provided no safeguard whatever regarding the permitted extent of the interference with the fundamental rights of the EU enshrined in the Charter.[88] In its judgment the Court of Justice formulated a number of proportionality requirements for which the directive made no provision at all. The judgment raises the question of the legal status of the laws enacted in the member states to implement the Data Retention Directive. The Advisory Division of the Council of State takes the view that the Telecommunications Data (Retention Obligation) Act remains valid, but must be brought into line with the requirements formulated in the judgment.[89] Germany has never implemented the directive and probably never will, because the Federal Constitutional Court has held that the implementing legislation is unconstitutional.

On 13 May 2014 the EU Court of Justice gave a landmark ruling in the Google Spain case on the privacy aspects of search engines.[90] In 1998 a Spanish newspaper had published a report that the applicant in this case (who was named in the report) had incurred debts and got into payment difficulties. In itself the message was correct. The paper version of the newspaper was later put on the internet. Sixteen years later, when typing in the name of the person concerned, the Spanish branch of Google put the report fairly high in the list of results displayed by the search engine. The person concerned

87 Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the US Terrorist Finance Tracking Program, Brussels, 16 March 2011, pp. 16-17. See: <http://ec.europa.eu/dgs/home-affairs/news/intro/docs/commission-report-on-the-joint-review-of-the-tftp.pdf>. On this subject see M. de Goede, 'The SWIFT affair and the global politics of European security', in *Journal of Common Market Studies*, 50(2), pp. 214-230.

88 Cases C-293/2012 and C-594-12, CJEU, 8 April 2014.

89 See: <http://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=287&summary_only=>.

90 Case C-131/2012, CJEU, 13 May 2014.

invoked the 'right to be forgotten' before the Spanish courts. It should be noted that he had applied to Google and not to the newspaper. The newspaper had taken no measures to ensure that the newspaper report could not be accessed by search engines, although this would have been technically possible.

What was at issue in this case was the application of the competency provisions of the Privacy Directive and the rule that the data subject could object on compelling grounds to the processing or further processing of data relating to him. In this context, the present provision for the right to erasure can be interpreted as a right to be forgotten. Google's head office in the United States and its Spanish subsidiary (Google Spain SL) had argued that this provision could not be applied because the processing of personal data (locating and indexing search results) occurred not in Europe but in the United States. However, the Court of Justice did not regard this as decisive. The economic operating model for the search engine is based on linking advertisements to search results. The advertisements are tailored to the national market in which Google's Spanish subsidiary operates. As Google Spain had in this case sold the advertisements in the Spanish market, the Court of Justice deemed this sufficient to hold that the directive was applicable. The processing of the personal data was carried out in the context of the subsidiary's activities, as stated in the directive. This part of the judgment is important because it shows that it is not easy for US companies and institutions to evade European privacy legislation if they operate within the EU. On this point, there is no difference of opinion about the fundamental significance of the judgment. What does give rise to debate, however, is whether the search engine should remove the personal data if they relate to a situation whose correctness or relevance is hard to check because of the lapse of time. The Court of Justice did not in any event take into account here the 2009 decision of the ECtHR in the Times Inc. case, which concerned article 10 ECHR and the importance of electronic archives on the internet being correct.[91] Erasing links to pages to ensure that they can no longer be found by the search engine limits the accessibility of historical sources available on the internet. The judgment in the Google case has generated a lot of debate because critics maintain that in applying the rules of the Privacy Directive, in combination with the relevant principles of the Charter, the Court of Justice failed to adequately balance the competing interests: privacy on the one hand and other rights protected in the Charter, in particular the freedom of expression and freedom to do business, on the other.

Quite apart from these issues, application of the judgment gives rise to practical difficulties such as how many search results must be erased and from which domains. An independent advisory body of the European Commission known as the Article 29 Working Party discussed this subject in July 2014 with the companies that operate the largest search engines.[92] A recent ruling on this issue by a Dutch interim relief judge balances the right to be forgotten against the need to ensure that historical information sources remain accessible.[93]

91 Times Newspapers Ltd. (nos. 1 and 2) v. the United Kingdom, nos. 3002/03 and 23676/03. See also *Nederlands Juristenblad* 2010, 109, with notes by E.J. Dommering.

92 See: <http://www.cbpweb.nl/Pages/pb_20140725_privacy-toezichthouders-zoekmachines-recht-om-vergeten-te-worden.aspx>.

93 Amsterdam District Court, 18 September 2014, ECLI: NL: RBAMS: 2014: 6118.

V Four categories of issues

This chapter describes four types of issues that have a bearing on the matters discussed above. 1. How will ICANN's multistakeholder model evolve? 2. The dilemmas of liberal democracies such as the United States and the Netherlands, which advocate freedom of the internet but at the same time permit more far-reaching internet surveillance for certain purposes. 3. The position of authoritarian states in the internet era. 4. The role of companies that operate internationally. The analysis of these issues must be brief in order to remain within the scope of this report.

V.1 The multistakeholder model and the roles that states, the private sector and NGOs can play in internet governance

The multistakeholder model

This model has widespread support, as will become apparent below. This was also demonstrated during the NETmundial meeting in Sao Paulo in April 2014, which was organised by the Brazilian government outside the context of the existing forums.[94]

The multistakeholder approach has various drawbacks.[95] First, it implies that all stakeholders can participate in decision-making on an equal footing. However, it would be an illusion to suppose that states and other stakeholders can have an equal say in decisions, if only because states have resources not available to other stakeholders. Equally, it is hard for states to participate openly in a free debate without giving the impression of having adopted an official standpoint. Corporate entities and non-governmental organisations (NGOs) have more freedom in this respect.

Second, stakeholders are, in practice, often divided into broad categories such as the private sector, states and NGOs. Within these categories, however, there may be a wide range of views. In such cases, the appointment of representatives in itself becomes a political process. Procedures to determine who can legitimately claim to represent a category of stakeholders can easily be manipulated.

Third, the multistakeholder approach simply means that the groups that will be affected by decisions are heard. In a national context, this is done within clear institutional frameworks by citizens who have clear rights and duties. For example, the Ministry of Economic Affairs carefully prepares the meetings of the Governmental Advisory Committee (GAC) within ICANN by consulting all stakeholders in the Netherlands. The Ministry does this because it considers it to be good practice, not because those concerned have a right of participation. In an international context, the situation is much more complicated. Important questions to be answered are who are the stakeholders, what are their rights and duties and who appoints representatives. In short, a multistakeholder approach requires at least some institutional infrastructure.

94 See: <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>, consulted on 26 June 2014.

95 M. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge, London: MIT Press, 2010, pp. 264-266.

Initially, the internet community challenged the established power of multilateral organisations and states, but now the groups that constitute the community have themselves become part of the establishment and defend their own interests and privileges, including huge salaries.[96] On the other hand, the absence of a formal structure means that policy competition exists between the different groups. This has in turn helped to generate a debate within ICANN about a Montesquieuan separation of powers.

Nonetheless, the multistakeholder model continues to have great appeal owing to the solidarity of the internet community and the binding factor of interconnectivity.[97] By their very nature, however, states, corporate entities and NGOs remain different kinds of entity. And their roles and functions therefore also differ, although they are often intertwined,[98] as will be explained below.

Democracies governed by the rule of law provide safeguards for their citizens and usually also advocate them in international organisations. Unlike companies and NGOs, states have to carefully balance competing interests. The internet has no boundaries, but the jurisdiction of a state is limited to its own territory. States can therefore safeguard national interests for the part of the internet within their jurisdiction, but this has its limitations as almost all internet traffic takes place across borders.

In many cases internet companies possess technical knowledge not available to other parties, which do not have the resources or motivation to make substantial investments in developing technical knowledge. An example is the developing and updating of antivirus software. This job can best be left to commercial organisations. Competition between providers of comparable services gives consumers freedom of choice and companies an incentive to deliver the best possible product. The disadvantage is that companies can acquire dominant positions in respect of vital parts of the internet and try to force through a process of appropriation in the open end-to-end environment.

NGOs can perform important functions such as developing norms. For example, they are often seen as the driving force behind the conclusion of the Ottawa Treaty, which bans the development, production, sale, stockpiling and use of anti-personnel mines worldwide. NGOs often conduct campaigns designed to focus attention on abuses or put questions on the political agenda. Some NGOs work in the public interest, and others represent the specific interests of their supporters (often members). Like corporate entities, NGOs lack democratic legitimacy, although they may represent values or interests which enjoy widespread support. In addition, most NGOs are established in Western countries.[99] NGOs in developing countries which receive funding from Western countries are increasingly discredited by the government of their own country and find it difficult, if not impossible, to perform their activities.

96 Idem, pp. 217-219.

97 See also: Laura DeNardis, *The Global War for Internet Governance*, New Haven and London: Yale University Press, 2014, pp. 226-227.

98 On the roles which companies and NGOs can play, see also: AIV, *The Role of NGOs and the Private Sector in International Relations*, advisory report no. 51, The Hague, October 2006, pp. 7-10.

99 Idem, pp. 30-31.

As noted in section II.2, the WGIG has formulated a working definition of internet governance. This reads as follows: 'Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.'[100] Countries that exercise control over the content of communications have a tendency to interpret this widely, as though it concerns the content of communications. The narrow interpretation is that it does not concern content. Nonetheless, the term can also be interpreted too narrowly. Van Eeten and Mueller[101] point out that in the scientific literature the term internet governance is often interpreted too restrictively as referring to ICANN and the influence of states. But even in the narrow sense internet governance includes more than this. Telecommunication policy too is relevant to internet governance since it includes regulation of the internet, competition policy and regulation of interconnectivity. Moreover, the addressing and domain name system, which are of huge commercial importance, must also be regarded as part of internet governance. Not only the technical but also the economic approach to internet security is important. The economic approach studies the incentives for actors to take or refrain from taking measures to enhance internet security. This can have consequences for anti-cybercrime measures and national security. Van Eeten and Mueller emphasise that internet governance takes place in an environment characterised by a low degree of formality, heterogeneous organisations, a multiplicity of actors and diffuse decision-making powers. Decisions are made not so much through a formal, central process as through the market, in networks based on trust, reputation and reciprocity and through 'peer production' (voluntary contributions by many autonomous actors) and crowdsourcing.[102] Van Eeten and Mueller point out that service providers which give access to the internet have also started playing a role in the security of the network and of customers' hardware, based on commercial considerations. Hitherto, this mix of organisational forms has functioned well.

ICANN's future

Much criticism continues to be levelled at ICANN's governance structure. As ICANN has a monopoly and is overseen by the US Department of Commerce, the US government can potentially exert more influence over an important element of the internet than other countries. Although ICANN has a Governmental Advisory Committee (GAC), membership of which is open to all states, many countries feel that they have insufficient control over ICANN.

In March 2014 the US government announced that it intended to transfer responsibility for the coordination of domain names to the global multistakeholder community and

100 Report of the Working Group on Internet Governance, June 2005, p. 4, point 10. See: <http://www.wgig.org/docs/WGIGREPORT.pdf>, consulted on 24 July 2014.

101 M. van Eeten and Milton L. Mueller, 'Where is the governance in internet governance?', *New Media & Society*, 15 (5), August 2013, pp. 720-736.

102 L.B. Solum, *Models* of internet governance, see: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136825>, consulted on 6 June 2014.

asked ICANN to hold public consultations on the desirable future structure.[103] In the announcement the Department of Commerce expressed the hope that ICANN would work with other major, long-established internet organisations such as the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB) and ISOC. The Department of Commerce also set conditions for the outcome of the consultation process. The proposal for transferring responsibilities must have broad support and satisfy the following criteria: (i) support and enhance the multistakeholder model; (ii) maintain the security, stability and resilience of the internet DNS; (iii) meet the needs and expectations of internet users; and (iv) maintain the openness of the internet. The Department also indicated that it would not accept a proposal for the responsibilities to be transferred to a government-led or intergovernmental organisation.

In the Montevideo Statement on the Future of Internet Cooperation (7 October 2013) the leaders of the main internet organisations called for accelerating the globalisation of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing. Among the signatories to the statement were the leaders of IAB, ICANN, IETF, ISOC and W3C.[104]

One of the most intractable issues is how and to whom a restructured ICANN or a new organisation should be accountable. The date by which the proposal should actually bring about change is not yet clear. In some ways the situation in which ICANN finds itself could be likened to that of the Republic of the United Netherlands in the 17th century, when it had just won its independence from the absolute power of the Spanish king and had to go in search of a new sovereign. The AIV notes that ICANN's future structure is a matter that deserves the government's close attention. The ICANN meeting in October 2014 set up a High-Level Team consisting of representatives of all stakeholders to formulate a solution. One of the points for consideration is whether ICANN can divest itself of two of its three functions (namely protocols and IP addresses), leaving it exclusively responsible for domain name management. A possible future place of establishment is Geneva, but everything is still under discussion. In the AIV's opinion, this too is something which deserves consideration by the government.

The importance of technical organisations for internet freedom

As noted above, a domain name has to be included in the root in order to reach the internet address in question, unless the website's IP address is known. In principle, ICANN records all domain names. A domain name can be removed in cases where continuation of the registration is incompatible with the legitimate interests of third parties. If authoritarian states could prevent the inclusion of domain names in the root, they could apply censorship not only in their own countries but worldwide. Although information unwelcome to these regimes could admittedly then be published under another domain name, the latter too would then be exposed to the risk of removal from the root. The end result would be that information unwelcome to these regimes would be difficult to find on the internet. Blocking a domain name could thus become part of a wider campaign to hinder or prevent access to certain websites. It is therefore important for control of the root to remain in neutral hands.

103 See: <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>, consulted on 25 June 2014.

104 See: <https://www.icann.org/news/announcement-2013-10-07-en>, consulted on 25 June 2014.

One of the most privacy-sensitive aspects of ICANN is its policy on the WHOIS databases for general top-level domain names. Every internet user can check a WHOIS database to find out who has registered a domain name and what the contact data are of the company or person concerned. Personal data can therefore be obtained from such a database. The Expert Working Group is researching ways of being able to supply information to law enforcement agencies and protect intellectual property rights while at the same time providing better privacy safeguards than in the current system. Some managers of country domains have already met all the objections, particularly in Europe. They display fewer personal data to the general public.[105] The WHOIS of the Dutch Internet Domain Registration Foundation, which registers domain names for the .nl country code domain, does not display the address data of the domain name holder. However, such data can be requested by bailiffs and attorneys. The Netherlands could also advocate such a solution internationally.

Open standards (open source software) can enhance the protection of the rights of internet users since it is then possible to check whether software incorporates backdoors, which make it possible to intercept and monitor data traffic. But there are also lobby groups which oppose this idea. The new internet protocol version 6 (IPv6 protocol) for the longer IP addresses contained a privacy protection, which was later removed.

The activities of W3C have a major impact on the privacy of users. Together, the World Wide Web and search engines make it possible to find information on the internet. When the World Wide Web was first introduced, websites and users' computers did not keep track of which pages had previously been visited. It was not possible for the website protocol to check from which computer (i.e. from which IP address) the website had been accessed. The protocol was modified in order to take advantage of the internet's commercial potential.[106] For example, a user wishing to place an online order for a retail purchase has to be able to switch from the store's website to that of the bank without the order being lost by the former. This marked the start of the behavioural targeting industry. By taking account of privacy considerations when designing the technical specifications, these organisations can play an important role in protecting internet freedom.[107]

W3C has taken various steps to protect the privacy of users.[108] For example, it has implemented the Platform for Privacy Preferences Project (P3P), which has resulted in a protocol that enables websites to inform the computer user's browser what data are being collected about the user. However, little use has been made of this protocol. In addition, W3C has published a proposal to enable users to determine for themselves

105 Lee A. Bygrave and Jon Bing, 'The naming game: governance of the domain name system', in: Lee. A. Bygrave and Jon Bing, *Internet Governance, Infrastructure and Institutions*, Oxford: Oxford University Press, 2009, p. 164.

106 Lawrence Lessig, Code version 2.0, New York: Basic Books, 2006, pp. 47-49. See also <http://codev2.cc/download+remix/Lessig-Codev2.pdf>, consulted on 16 June 2014.

107 Laura DeNardis, *The Global War for Internet Governance*, New Haven and London: Yale University Press, 2014, pp. 78-79.

108 Idem, p. 79.

what data can be collected about their behaviour on the internet. It is desirable for the United States (as the country in which many major internet companies are based), the EU and other Western countries to consult with W3C about how the use of such protocols can be promoted and what role governments and W3C can play in this.

The Internet Governance Forum

The IGF plays a useful role, but is hampered by a lack of manpower and resources. This detracts from the preparation of the meetings. As a result, the agenda is largely determined by states, corporate entities and institutions that do provide funds. The differences of opinion about internet values also make it difficult for the IGF to adopt strong common norms (see chapter II). Another problem is that some major players such as Google and Facebook are not represented. The AIV recommends that Dutch participation in the IGF be strengthened by allocating a larger budget and ensuring that organisations in the field are properly consulted in preparation for IGF meetings.

V.2 The dilemmas facing Western democracies: the United States and the Netherlands

The dilemmas outlined below come about because although the constitutional democracies of the West advocate and indeed achieve a very high level of public and private freedom of communication, they are at the same time taking advantage of the almost unlimited technical possibilities for monitoring to gather more and more data to contend with the permanent terrorist threat. This is allowing greater oversight of private life and communication, thereby jeopardising uninhibited communication and the right to respect for private life. If democracies are unable to reconcile these two aspects in accordance with the rule of law, they are in danger of being seen by the world as Janus-faced, paying lip service to one set of values while actually implementing another. Owing to differences between the Dutch and US legal systems, these countries are tackling these dilemmas differently. How this is done in each of these countries is described below. The situation in the United States is also important to the Dutch because it is also home to the largest internet companies (social media, search engines and clouds).

V.2.1 The United States

Internet freedom

Section IV.1 referred to the International Covenant on Civil and Political Rights, articles 17 and 19 of which deal with the right to privacy and the right to freedom of expression respectively. The United States interprets article 2 of the Covenant[109] as though only persons within its territory and subject to its jurisdiction are entitled to the rights mentioned in the Covenant.[110] This principle is still applied because at the time of ratification the reservation was made that the provisions of the Covenant are not self-executing. In recent years there has been an ongoing debate about the universal value of the rights guaranteed in the Constitution, with particular reference to the principle

109 'Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.'

110 CCPR/C/USA/4, 30 December 2011, pp. 142-143.

that only US citizens and residents are entitled to the protection of the Constitution.[111] There are signs that this position is shifting, partly as a result of the Snowden affair. The President has announced measures in this field.[112]

Owing to the First Amendment, the United States has always played a leading role in the world in respect of the freedom of expression, including on the internet. The United States was fairly quick to recognise that the internet was a medium that would have an important bearing on the freedom of expression. In a series of decisions starting with Reno v. ACLU,[113] the principle of the effective protection of press freedom on the internet was applied and filter measures were usually condemned. The measures which the United States considers permissible in the interests of national security are at odds with this tradition. The Snowden affair has revealed this more clearly than ever.

The US Constitution makes no provision for an independent right to privacy. This right is mainly derived from the Fourth Amendment, which protects citizens from unreasonable searches and seizures. Owing to the source of this provision, it cannot be applied to the private sector. However, there is a Privacy Act, which is applicable only to the public sector. Data which have been voluntarily communicated to businesses may be used by them for other purposes without the consent of the data subjects. In addition, various statutes contain privacy provisions. Privacy provisions may be set aside for reasons of national security. There are no data retention rules that oblige companies to retain data.

The United States has a data protection system that differs significantly from the systems in force in the EU and many other countries. Instead of a general data protection statute binding on the private sector, it has much sectoral legislation. As not all sectors have legislation there are gaps. Nor is there a data protection authority to supervise compliance with the legislation.[114] Only a small number of statutes limit the quantity of data which companies may collect. Moreover, in the unregulated sectors businesses may also use personal data for all kinds of purposes without the customer's consent. They need not inform customers of this use or provide them with any means of preventing this. By contrast, EU legislation states that for all sectors data may be collected, processed and used only for a predetermined purpose and gives people more control over the data after they have supplied them. The differences between the United States and the EU create tensions in the transatlantic exchange of data, with the EU making demands about the level of protection which can hardly be met by the United States (see section IV.3.2).

111 David Cole, 'Are foreign nationals entitled to the same constitutional rights as citizens?', *T. Jefferson Law Review*, no. 25, 2003, pp. 367-388.

112 Presidential Policy Directive, Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435, 17 January 2014, see: <http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>, consulted on 16 June 2014.

113 521 US 844 (1997).

114 Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, University of Edinburgh School of Law, Research Paper Series no. 2012/12, pp. 3-6.

Privacy and intelligence and security services: Snowden

In 2002 the US Defense Advanced Research Projects Agency, which was involved in the birth of the internet, established the Information Awareness Office to achieve 'Total Information Awareness' (TIA). Following the September 11 attacks, the TIA programme was converted into a programme for a counterterrorism information infrastructure. As this completely lacked any statutory basis, the Senate (and later the House of Representatives) withdrew funding from the TIA in 2003. Although this officially marked the end of the TIA programme, it actually continued under another name. In 2007 the NSA transferred the project – under the name of PRISM – to a special source operation, which had been started in 1970. The NSA works with around 100 US trusted companies in this operation.

Snowden revealed, among other things, that the NSA had engaged in the mass collection and storage of the telephone metadata of US citizens. From 2006 onwards this had been done on the basis of section 215 of the USA PATRIOT Act (2001). Thereafter it was continued subject to annual review of certifications by the Foreign Intelligence Surveillance Court (FISC). The FISC prohibited the NSA from applying data mining techniques to the traffic data. Instead only targeted searches could be made. In addition, the NSA collected the content of communications, including telephone calls and emails, of persons assumed to be foreigners and not present in the United States. The legal basis for this is section 702 of the FISA Amendments Act (2008).

Following the Snowden revelations, the US President established the President's Review Group on Intelligence and Communications Technologies, which reported to the president in December 2013.[115] In addition, the US Privacy & Civil Liberties Oversight Board (PCLOB) published two reports, one about section 215 and the other about section 702.[116] The reports do not touch on other NSA programmes alleged to exist by Snowden, including the allegations that the NSA had cracked the encryption of messages (using the Bullrun decryption program) and had discovered and exploited weaknesses in corporate programs or even had them built into the programs, thereby enabling it to hack computers.[117]

The issue of the legal permissibility of the NSA's activities is assessed in these reports from the perspective of the US Constitution and legislation. The Presidential Review Group makes only passing mention of human rights.[118] The report of the Presidential Review Group and that of the PCLOB on section 702 describe in detail the legal rules for intercepting communications of foreigners located outside the United States. These

115 *Liberty and Security in a Changing World*, *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, December 2013.

116 Privacy & Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, January 2014, and *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 July 2014.

117 See: <https://www.eff.org/nsa-spying>.

118 *Liberty and Security in a Changing World*, *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, December 2013, p. 155.

differ in some important ways from those governing the interception of communications of American citizens and persons lawfully present in the United States, whose rights are protected by the Fourth Amendment.[119] To carry out a targeted investigation relating to members of this group, the government needs probable cause and an individual warrant. Neither of these conditions applies to foreigners outside the United States, even where the communication is intercepted in the United States. Instead of a probable cause, the government only needs a reasonable belief that an email address or telephone number is being used for the purposes of international terrorism, nuclear proliferation, hostile cyber activities and so forth.[120] This means that much less protection is afforded to the confidentiality of communications and the privacy of foreigners outside the United States than to those of Americans and foreigners located in the United States. The Presidential Review Group recommends that foreigners be given the same rights (rights to access records, rights to make corrections and legal remedies) as possessed by US citizens and residents under the Privacy Act, even in relation to the intelligence and security services, in the absence of a compelling reason for not doing so. This would formalise the approach taken by the Department of Homeland Security.[121] On 25 June 2014 Attorney General Eric Holder gave an undertaking to the European ministers of justice and home affairs that the US government would present a bill to Congress to extend the operation of the Privacy Act to EU citizens.[122] European citizens would then obtain the same rights as US citizens to seek judicial redress for intentional or wilful disclosures of protected information. Evidently, the proposed expansion of the operation of the Privacy Act would not apply to other foreigners. As noted previously, the level of protection of privacy in the United States is in some ways substantially lower than in the EU.[123]

The reports of the Presidential Review Group and of the PCLOB on section 215 of the USA PATRIOT Act address the question of the extent to which the collection of bulk telephony metadata of US citizens is lawful under the US Constitution and US law. Views differ on this point. According to the Review Group, it is necessary to decide whether the additional safety achieved through the collection and storage of bulk metadata is worth the sacrifices in terms of individual privacy, personal liberty and public trust.[124]

119 The text of the Fourth Amendment: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

120 *Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, December 2013, pp. 152-153.

121 Idem, p. 157, recommendation 14.

122 *The Guardian*, 25 June 2014. See: <http://www.theguardian.com/world/2014/jun/25/us-privacy-protection-rights-europe>, consulted on 26 June 2014.

123 Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108?*, University of Edinburgh School of Law, Research Paper Series no. 2012/12, pp. 3-6.

124 *Liberty and Security in a Changing World*, *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, December 2013, pp. 108-114.

The reports deal with the issue of the extent to which these programmes were effective. Both the PCLOB and the Presidential Review Group conclude that the collection of bulk telephony metadata under section 215 was not effective in preventing terrorist attacks. In so far as the programme yielded relevant information, this could also have been obtained by less intrusive methods.[125] The PCLOB points out that the idea that the government could misuse stored information is by no means fanciful, given the recent history of the United States. Moreover, the collection and storage of metadata by the government may make people wary of expressing their views, because the confidentiality of information is not guaranteed.[126] However, one member of the PCLOB did consider the programme to be effective.[127]

V.2.2 The Netherlands

The Netherlands leads the way in promoting internet freedom. As noted in the request for advice, the Netherlands established the Freedom Online Coalition. This achieved success at the ITU World Conference on International Telecommunications in Dubai, by preventing the proposal to amend the International Telecommunications Regulations to increase government surveillance of the content of communications (see section II.3). The Netherlands is taking active steps to respond to the European Commission's Green Paper entitled 'Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values'.[128]

The Netherlands has a sizeable internet-related industry. For example, Amsterdam is home to the world's largest internet exchange (AMS-IX, with over 600 connected networks). The country's digital infrastructure sector has a turnover of approximately €1.5 billion and is estimated to account for approximately one third of European turnover in e-commerce. It is also an important growth sector.[129]

Just as in the United States, examples can be found in the Netherlands of the manifest dilemma between a very large degree of public and private communication freedom and the increased collection of data related to private life and uninhibited communication. The Dutch too are struggling to strike a balance between privacy and national security within the framework of the rule of law.

125 Privacy & Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,* January 2014, p. 146, and *Liberty and Security in a Changing World*, *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, December 2013, p. 104.

126 Privacy & Civil Liberties Oversight Board*, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, January 2014, pp. 155-164.

127 Idem, Annex B.

128 Green Paper, *Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values*, Brussels, 24 April 2013, COM(2013) 231 final. For the draft reaction of the Netherlands, see House of Representatives of the States General, 22112, no. 1659, with annexe.

129 Figures taken from *The.nlyst,* no. 15, Q3 2014, a publication of the Internet Domain Names (Netherlands) Foundation.

It was explained in section III.4.1 that the metadata on an individual can shed much light on his or her behaviour and preferences. However, the distinction between content and metadata is not sharp. This question is of relevance, for example, to the revision of article 13 of the Dutch Constitution. It is apparent from the explanatory memorandum to the bill and from the further report (in response to the Council of State's advisory opinion) that the government does recognise that the distinction has become blurred, but considers that this does not mean that all traffic data deserve the same level of constitutional protection as the content of the communication. The explanatory memorandum to the bill to amend article 13 mentions various borderline cases between content and traffic data and explains that it has been decided that traffic data relating to the content of the communication should be covered by the right to respect for the confidentiality of telecommunications. This will be framed in more detail by the legislator and the courts.

After the European Data Retention Directive was declared invalid in April 2014, the Minister of Security and Justice sent his reaction to the House of Representatives of the States General on 17 November 2014, following consultation with the Advisory Division of the Council of State.[130] The Minister and the Advisory Division concluded that although the directive had been struck down this did not mean that the Dutch legislation too was invalid. The Minister stated that the relevant legislation must be adjusted in various respects to bring it into line with the data retention requirements set by the EU Court of Justice. For example, there must be prior consent by an examining magistrate for the collection of telecommunication data, differentiation of access to data according to the gravity of the offence, possible encryption of stored data, compulsory storage in the territory of the European Union and expansion of the powers of the Radiocommunications Agency Netherlands to ensure stronger oversight.

The AIV considers that the collection of bulk telephony metadata is not permissible as it breaches the right to privacy, except where there are statutory rules that meet the conditions of the fundamental rights concerned. In its judgment declaring the Data Retention Directive to be invalid the EU Court of Justice indicated what conditions the storage of metadata should fulfil. In his letter to the House of Representatives of the States General, the Minister of Security and Justice gave an undertaking on behalf of the government to take this judgment into account when reviewing the Intelligence and Security Services Act (WIV) 2002.[131]

In its report no. 38, the Intelligence and Security Services Review Committee (CTIVD) notes that technological advances are making it possible to exercise powers in ways not foreseen by the legislator. Although these ways are not, strictly speaking, in breach of the WIV, the safeguards are inadequate. This applies, for example, to the analysis of metadata. The CTIVD recommends that a specific provision regulating the analysis of metadata should be included in the WIV since they can, in part, be defined as personal data. The CTIVD also recommends that a maximum period for the storage of raw data should be included in the WIV. The government has adopted both recommendations.[132]

130 House of Representatives of the States General, 33 542, no. 16.

131 Idem, p. 14.

132 House of Representatives of the States General, 29 924, no. 105.

On 21 November 2014 the government informed the House of Representatives of its views on revision of the interception system under the WIV. The government has accepted the recommendation of the Dessens Committee that the distinction between cable-bound and non-cable-bound communications should be dropped and additional safeguards included in the legislation.[133] Sections 26 (exploration of communications) and 27 (untargeted interception) of the WIV will be amended to extend the powers of the intelligence and security services to cable-bound communications. The actual processing will take place in three stages, each of which will have its own safeguards. Although the government has given a broad indication of the nature of these safeguards, no specific information is available. The letter makes no reference to the judgment of the EU Court of Justice in which the Data Retention Directive was declared invalid and the requirements for the storage of data were set out. As the same safeguards will apply to the interception of cable-bound and non-cable-bound communications, the level of protection for the latter will be enhanced.

The government has not adopted the Dessens Committee's recommendation that the body responsible for external oversight of the intelligence and security services should be able to issue binding and timely instructions about the lawfulness of the surveillance and investigative activities. This recommendation was supported by the CTIVD. The government notes that the minister is fully responsible at all times for the operational activities of the services and is also fully accountable for them to the two houses of parliament. If the CTIVD discovers activities which it believes should be stopped forthwith, it may inform the minister accordingly. The CTIVD's recommendation is a matter of public record for which the responsible minister can thus be held politically accountable.[134]

A number of civil liberties organisations have instituted legal proceedings in the Netherlands about the cooperation between the Dutch intelligence and security services and the NSA. After the case was dismissed on the facts at first instance, the plaintiffs have now lodged an appeal.[135] Each year the Ministry of Security and Justice publishes information about the number of telephone and internet taps. It has also established a working group to study whether greater transparency can be provided about wire tapping and, if so, how.[136]

It should also be noted that a Computer Crime III Bill will shortly be presented to parliament.[137] The draft submitted for consultation shows that the legislation will introduce far-reaching powers to help combat computer crime. Of particular relevance here is the proposal to give the police the power to hack computers. Basically, the bill will allow the police to install malware in a suspect's computer or smartphone, thereby

133 House of Representatives of the States General, 33 820 no. 4.

134 Idem, 33 820, no. 2, p. 6.

135 The Hague District Court, 23 July 2014. See: <http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:8966>.

136 See: <http://over.vodafone.nl/nieuwscentrum/nieuws/actueel-nieuws?page=5>, consulted on 12 November 2014.

137 See: <http://www.internetconsultatie.nl/computercriminaliteit>.

enabling them to search the hard drive covertly, log keystrokes and activate the camera and microphone remotely. The bill has received a critical reception,[138] not only because it will create many possibilities for remotely monitoring every aspect of a suspect's life but also because it proposes that the powers should be exercisable across borders. This could occur when the place where data are stored is not known (a very likely scenario in the case of cloud computing), but the bill does not actually exclude the possibility that even when the place of storage is known, information may be searched for and made inaccessible from the Netherlands, without the prior consent of the other state. The unsubstantiated statement in the explanatory memorandum to the consultation version of the bill[139] that this is in conformity with international law is disputable. In the AIV's opinion, trans-border access to computers without the consent of the state in which the data are stored is not permitted under international law as it stands.[140] Clearly, this is unsatisfactory, given the need for effective powers to investigate cybercrime. Although the standard procedure of requesting mutual assistance in criminal matters is far too time-consuming in cases where the aim is to secure transient data, this does not detract from the legal limits currently set by international law. In its current form, the bill might also harm the status of the Netherlands in the international community as a champion of internet freedom and deprive it of the ability to complain under international law if foreign states were to hack into Dutch computers to copy corporate data. Rather than unilaterally introduce a trans-border power, the Netherlands could better await and actively support the proposal for an additional protocol to the Convention on Cybercrime concerning trans-border access to data for investigative purposes. This is something which the Ministry of Security and Justice is already actively promoting.

Besides the trans-border dimension, it should also be noted that the bill authorising the police to hack into computers constitutes an exceptionally far-reaching infringement of the right to respect for privacy – an infringement which goes much further than admitted in the draft explanatory memorandum to the bill. This is because a remote search of a computer or smartphone yields much more information about a person's private life than a traditional search of premises. In a recent landmark judgment about mobile phone searches, this was formulated by the US Supreme Court as follows: 'A cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form. (…) With all they contain and all they may reveal, they hold for many Americans "the privacies of life".'[141] A police power to hack into computers and

138 C. Conings and J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?' (Network searches and online investigations (jurisdictional issues)), *Computerrecht*, 2013, no. 1, pp. 23-32.

139 Computer Crime III Bill, explanatory memorandum, p. 36, available at <http://www.internetconsultatie.nl/computercriminaliteit>.

140 An exception applies to states which are parties to the Council of Europe's Convention on Cybercrime in cases covered by article 32 (b). This provides that the authorisation of the other state is not required if the lawful and voluntary consent has been obtained either of the person who has the lawful authority to disclose the data or of the internet provider who has lawful access to the stored data.

141 Riley v. California, 573 U.S. _ (2014). See: <http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>.

smartphones is therefore compatible with the right to privacy only if it is hedged around with strict proportionality and subsidiarity safeguards.

The AIV would draw the government's attention to the fact that the policy issues discussed above must be viewed in the light of the resolution adopted by the UN Human Rights Council in July 2012 on the promotion, protection and enjoyment of human rights on the internet (A/HRC/20/L.13) and to the desire of the Netherlands to lead by example, especially on human rights. This is not just about whether and, if so, for how long lesser degrees of protection for fundamental rights are defensible within the international legal order but also about whether the Netherlands wishes to be at the forefront of the efforts to move the legal order in the desired direction.

V.3 Censorship, control and the mobilising function of the internet

Although China and Russia have been selected here as examples of censorship and control of the internet, many other examples could be given. The efforts of these countries are directed in various ways towards transforming the internet into an intranet (in China by means of a digital Chinese Wall), with incoming and outgoing traffic being routed through central servers, national traffic being heavily censored for content, and user behaviour and communications being strictly monitored.

The following observations can be made on the basis of the criteria developed by Freedom House and quoted in chapter 1.

China[142] *and Russia*[143]

Although China has not ratified the International Covenant on Civil and Political Rights, it has signed it and must therefore refrain from acts that would defeat or undermine its objective and purpose. By contrast, the Russian Federation has ratified the Covenant. Moreover, it is a member of the Council of Europe and is thus subject to the provisions of the ECHR and the judgments of the ECtHR.

The constitutions of both China and Russia guarantee freedom of expression, but in practice civil and political rights are limited. Justification for the limitations is usually sought in arguments based on state security or state secrets legislation (China) or extremism legislation (Russia). As this legislation is vaguely worded, the authorities have a wide discretion in applying it and citizens have little legal certainty. The government uses instruments such as propaganda and censorship to buttress the position of the governing party, both generally and online. When the internet was first introduced in China

142 Freedom House, *Freedom of the Press 2013*, pp. 120-127. See: <http://www.freedomhouse.org/sites/default/files/FOTP%202013%20Full%20Report.pdf>, Freedom House, *Freedom in the World 2014*, <http://www.freedomhouse.org/report/freedom-world/2014/china-0> and Freedom House, Freedom on *the Net 2013*, see: <http://www.freedomhouse.org/report/freedom-net/2013/china>, all consulted on 10 July 2014.

143 Freedom House, *Freedom on the Net 2013*, pp. 588-600, Freedom House, *Freedom of the Press 2013,* pp. 315-319, <http://www.freedomhouse.org/sites/default/files/FOTP%202013%20Full%20Report.pdf> and Freedom House, *Freedom in the World 2014*, see: <http://www.freedomhouse.org/report/freedom-world/2014/russia-0>, all consulted on 10 July 2014.

in 2001, its then leader President Jiang Zemin described it as 'a political, ideological and cultural battlefield'.[144]

The main censorship method is to apply automatic filtering, but information is also removed manually from the internet. Government agencies in both countries draw up lists of websites to be blocked by internet service providers, without any form of judicial review either before or after the decision. In China, internet service providers can be held liable for distributing information that is unwelcome to the authorities. They therefore apply self-censorship. Nonetheless, the authorities are not always able to block or remove unwelcome information before it becomes widely distributed. International internet service providers do not always cooperate. For example, Google attempted to evade censorship in 2010 by referring internet users in China to the uncensored search engine operated on servers in Hong Kong. It should be noted that not all political criticism is censored; the emphasis is on censorship of statements which call for or may lead to mobilisation of groups or other collective action.[145]

New rules for the registration of domain names with the .ru country code domain took effect in Russia in late 2011. Certain law enforcement authorities have the power to issue written instructions for termination of the registration of specific domain names, which means that they in fact cease to exist. Another way of preventing access to content is to mount distributed denial-of-service attacks on websites. Since May 2014 bloggers who have more than 3,000 followers have a duty to register with the authorities. Social media are being subjected to increasingly strict (informal) control.

From 2016 Russia will have a statutory data localisation obligation that requires the personal data of Russian citizens to be stored in databases in Russia.[146]

In addition, the authorities of both Russia and China manipulate content on the internet by paying bloggers to post positive comments about government officials, the ruling party and government policy. In Russia the activities of these 'trolls' are becoming increasingly noticeable.

Privacy protection is limited in China. There is no relevant constitutional provision and there is no law on privacy. Although there is a constitutional provision on the privacy of correspondence, this is subject to many exceptions.[147] Nor does China have a general data protection statute.[148]

144 Evan Osnos, *Age of Ambition, Chasing Fortune, Truth and Faith in the New China*, London: The Bodley Head, 2014, p. 30.

145 Gary King and others, 'How censorship in China allows government criticism but silences collective expression', *American Political Science Review*, May 2013.

146 'Gegevens over de toenemende internetrepressie' (Data on Growing Internet Repression), Tanya Lokshina, programme director of Human Rights Watch, Moscow, *Volkskrant*, 2 August 2014.

147 UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, 2012, pp. 74-78. See: <http://unesdoc.unesco.org/images/0021/002182/218273e.pdf>.

148 Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108?*, University of Edinburgh School of Law, Research Paper Series no. 2012/12, p. 6.

In China access to foreign internet services such as Facebook, Twitter and YouTube is blocked. Filters prevent access to the services from China. Chinese companies have created national versions of the services, which have proved highly popular.

Various technical methods can help users to avoid censorship, for example sending prohibited information through peer-to-peer networks or virtual private networks. Another method is to use homonyms. This capitalises on the fact that even slight changes of pronunciation can give Chinese words an entirely different meaning. The Internet Affairs Bureau in Beijing uses its massive manpower in a continuous but virtually hopeless struggle to limit freedom of expression on the internet.[149]

The lack of internet freedom is an aspect of the broader democratic deficit and deficiencies of the rule of law in authoritarian countries. Internet censorship is therefore supplemented by repressive measures, such as detention of popular bloggers. Administrative or tax measures are increasingly used to silence human rights activists.

The mobilising function of the internet

During the upheavals in the Arab world, much was written about the role of social media. Unemployment, poverty and political exclusion were the main reasons why the relatively young, better educated and articulate population rose up in rebellion.[150] Social media have played an important role in the political developments in the Arab region because they have contributed to the rapid dissemination of information, increased political awareness and provided a platform for networks and mobilisation.[151]

Social media can help to counterbalance government propaganda, especially in situations where the government controls the other media. Provided they are not under government control, social media provide an easier route for formulating alternative narratives. Although they can serve as a platform for debate, they can also be used to disseminate misinformation and propaganda.

Before the internet existed, various abuses were known only locally or nationally. Now, however, a single incident can quickly acquire worldwide notoriety through social media and prompt mass public protests against the authorities. Examples are the Facebook campaign following the death of the Khaled Saeed in Egypt as a consequence of police violence in June 2010, and the self-immolation of the Tunisian street vendor Mohammed Bouazizi in December 2010. Social media also make it possible to tell the whole world about important events while they are happening. For example, an artillery bombardment of the Syrian city of Homs could be followed on the internet while it was happening.

As social media make it possible to reach many people simultaneously they are an effective way of mobilising support, even if the recipients are geographically remote from one another. A call to demonstrate can be sent to many people in the blink of an eye. In the Russian Federation opposition leader Alexei Navalny used social media to collect

149 Evan Osnos, *Age of Ambition, Chasing Fortune, Truth and Faith in the New China*, London: The Bodley Head, 2014, pp. 199-203.

150 AIV, *The Arab Region: An Uncertain Future*, advisory report no. 79, The Hague, May 2012.

151 Paul Aarts and others, *From Resilience to Revolt, Making Sense of the Arab Spring*, University of Amsterdam, June 2012, pp. 45-47.

money for his movement and win votes for his bid in the Moscow mayoral elections in September 2013.[152] However, although social media can help to mobilise people, other conditions must also be fulfilled if people are to be induced to become politically active.[153]

Governments of countries where the freedom of expression is under threat fear the use of social media to mobilise people. They seek to control these media by imposing statutory restrictions on users and companies and by exerting pressure on companies and obliging them to cooperate with censorship. Most states do not succeed in preventing all undesired content since the volume published is simply too much. If the threat becomes too great, the authorities sometimes shut down the internet for a short period. But in almost all countries the economic importance of the internet is such that it cannot be closed down for long. Alibaba, the Chinese equivalent of Amazon, was responsible for one of the largest stock market flotations in history when it made its debut in the United States in September 2014.

Broadly speaking, there are two ways of promoting freedom of expression on the internet. The first is to press for better compliance with existing rules. The second is to create technical means for human rights activists to avoid censorship and other obstacles. The experts consulted by the AIV stated that the technology is available, but needs to be made more user-friendly. The Dutch government supports various activities of this kind, such as training bloggers and online journalists about censorship avoidance techniques and about online and offline security. The Netherlands was one of the founders of the Freedom Online Coalition in 2011.

V.4 The role of the private sector

Reference was made in section III.3 above to the role of intermediaries who enjoy protection from government interference in democracies governed by the rule of law. It was also noted that the protection for the role of these intermediaries has not yet been formalised in legislation. If the authorities wish to curb internet freedom they must observe the principles of the rule of law in respect of both users and internet companies. The extent to which companies pursue an active policy on internet freedom differs. Some have procedures and policies in place for the removal of content. They may or may not oppose requests by the authorities for the removal of content or the disclosure of information to the authorities. At present, proceedings in which Microsoft disputes the competence of US federal authorities to order it to disclose the contents of an email held on a server in Ireland are under way before a US court. Microsoft is supported in this by other large American internet companies.

Internet companies also have their own views on what is and is not permissible, for example in relation to moral issues. Transparency about the extent to which they filter content differs from company to company. Twitter informs users about blocking, but Facebook does not. The far-reaching cooperation between internet companies and the NSA in the context of PRISM is very opaque as the companies have a non-disclosure obligation. As internet equipment and services usually contain secret source codes, it

152 Freedom House, *Freedom in the World 2014*, Russia, p. 1.

153 Paul Aarts and others, *From Resilience to Revolt, Making Sense of the Arab Spring*, University of Amsterdam, June 2012, pp. 34-38 and pp. 45-47.

is unclear to what extent there are technical leaks which can jeopardise the privacy and security of users.

In less democratic countries the authorities often put pressure on internet companies to make websites unfindable, filter content, remove tweets, disclose information about the identity of bloggers and so forth. Even international companies may experience pressure and have to balance their commercial interests against human rights owing to the absence of legal remedies. If international companies choose to continue their business operations in countries that have low standards of internet freedom, they can still try to be transparent about the extent to which they cooperate with censorship. For example, they can publish statistics about the number and nature of warrants they receive from the authorities. They can also inform the affected users. However, this may be prohibited. This is why some companies send their customers a 'warrant canary', which is a (permissible) communication that the provider has not yet received a secret warrant to disclose data about the customer.[154]

International internet companies respond in different ways to requests from authorities to filter or manipulate content.[155] For example, Google Maps presents different borders of Ukraine to different audiences, depending on where they are in the world. Google decided to do no further business in China after it had been ordered to filter results. Twitter complies with requests from authorities to remove tweets, but only blocks the tweet for the country concerned. In other countries the tweet remains visible. By modifying results locally, a company can continue operating in countries where freedom of expression is limited, but in doing so it is complicit in censorship. This detracts from the function of the internet as a platform for debate. As the content in the rest of the world remains visible, internet users in other countries are informed.

Given all these conflicting positions, it would be difficult to use the private sector as an instrument for promoting the human rights policy advocated by the Dutch government. Much is already being done in this field, as is shown by the UN's Guiding Principles on Business and Human Rights (known as the Ruggie Principles after their author).[156] The special urgency in the communications field is because the worldwide public and private communication channels and services are in the hands of these companies. A policy on these communication companies has a chance of success only if coalitions are formed in international forums. An example is the Snowden case, where there is a growing European consensus that the PRISM Programme cannot be continued in its present form since its violates the rights of Europe's citizens. Nonetheless, the AIV considers it desirable to formulate a policy in which companies operating in the Netherlands are encouraged to respect Dutch human rights policy. There does not appear to be any good reason why the Netherlands should maintain a human rights dialogue with authoritarian countries but not with companies which are essential to the maintenance of privacy and the freedom of communication in the world.

154 See: <http://en.wikipedia.org/wiki/Warrant_canary>.

155 See: <http://gigaom.com/2014/05/21/twitters-selective-censorship-of-tweets-may-be-the-best-option-but-its-still-censorship/>.

156 A/HRC/17/31.

VI Summary, conclusions and recommendations

Summary and conclusions

Chapter II explains that the internet, as represented by the internet community, has broken free of the traditional structure of the telecommunication sector under international law, namely a convention (recording global agreements about telecommunications) and an international organisation (the International Telecommunication Union) in which national states work together. This structure has been replaced by a multistakeholder model, partly under private law, consisting of ICANN (domain names and addressing) and a range of technical groups that regulate the internet's standards and protocols. This change has been accompanied by a technical revolution in the manner in which data are transmitted and a social revolution in the manner of communication. ICANN still has formal ties with the US Department of Commerce. The prevailing view since the Snowden affair is that these ties can no longer be maintained. Ways of basing a new structure on the multistakeholder model are now under consideration.

This form of governance is limited to the technical layers of the digital network, although there is no consensus within the internet community about this narrow interpretation of governance (see section V.2). Alongside this new internet structure, an old organisation – the ITU – is still trying to extend its sphere of influence, most recently by an attempt to modify the International Telecommunications Regulations at the World Conference on International Telecommunications in Dubai. Hitherto, its efforts have been unsuccessful. Within the ITU, countries such as Russia and China are attempting to get a tighter grip on internet communications, including content. Some time ago, however, the UN established a new global organisation known as the Internet Governance Forum (IGF). In this framework, states are attempting to cooperate with other stakeholders to reach consensus on the concept of internet governance. Hitherto, this has met with only partial success because, quite apart from the more technical issues, it is very difficult to reach consensus on subjects about which the parties hold such widely differing views. This is the background against which the AIV has answered the government's questions.

The government's first question was how can it ensure that internet freedom is embedded and further operationalised in Dutch domestic and foreign policy as effectively as possible. This question has been discussed at a conceptual level in chapter III. First, it is explained that the existing framework of communication and privacy-related fundamental rights is no longer in keeping with the current state of the technology. It is also apparent that any measures to change this should be taken only after proper consideration and with due caution, in order to avoid lowering the level of protection. This is demonstrated by reference to factors such as traffic data and the privacy of communication. Privacy of communication is no longer a static given in a network society, but is instead about the protection for how and in what connection an individual can communicate freely. A second important point is that the legal concepts have either been developed for a technical reality different from the current internet (e.g. the concept of processing in data protection law) or are based on a situation in which a clear distinction can be made between the transport and expression of the message (from media and telecommunication law). Another important and related question concerns the divide between international jurisdiction and the universality principle on the one hand and national sovereignty on the other. This divide is reflected, above all, in the difficult negotiations between the EU and the United States on the safe harbour principles in

relation to data protection. Another matter deserving consideration is the ongoing erosion of the concept of personal data due to developments such as Big Data and the mass or targeted surveillance of citizens. Many people wrongly assume that traffic data are not, by definition, personal data, but it has to be realised that individual profiles can be compiled from a collection of traffic data. So the assumption that it is acceptable for anonymous data to be collected on a massive scale without effective supervision is also incorrect.

It is also noted that security should be viewed in the context of the rule of law. Striving to achieve the impossible ideal of precluded event security can lead to the adoption of disproportionate measures that harm the balance under the rule of law.

This advisory report also describes the clash of views on the broadening of the definition of internet governance, which has a bearing on the embedding of internet freedom in domestic and foreign policy. One of the places in which this clash is most visible is the ITU (section II.3). The debate about the new organisation to replace ICANN is also of great importance because control of the root is critical to internet freedom and ICANN can be seen as the spider at the centre of the internet governance web (section V.1). The Internet Governance Forum (IGF) appears to be a suitable organisation in which to debate issues connected with the operationalising of internet freedom, but its secretariat is understaffed and underfunded.

The government can also make a contribution to promoting internet freedom by applying the same normative principles in policy debates in the Netherlands as it advocates abroad. If constitutional democracies fail to do this, they risk being seen by the world as Janus-faced, paying lip service to one set of values (the rights and freedoms guaranteed under the rule of law) while actually implementing another (restrictions on freedoms that do not meet the safeguards required under the rule of law), as explained in section V.2. This is the very problem which is currently detracting from the credibility of the United States at home and was criticised by Richard Haass, president of the US Council on Foreign Relations, in his study entitled Foreign Policy Begins at Home.[157]

The second question was whether Dutch jurisdiction over internet freedom is limited to activities in the Netherlands, or whether it extends, by virtue of the increased technological possibilities, to situations outside the country. The second part of the question was how the Dutch government could help to effectively safeguard internet freedom beyond the country's borders if such jurisdiction does not extend this far. On the internet the production, storage and distribution of information is no longer bound by place and time. The internet has no national borders. However, although the technological possibilities have indeed increased, this does not mean that the powers too are broader. In section V.2.2 this question is focused on the draft of the Computer Crime III Bill which has been the subject of consultation. In the AIV's opinion, the powers created in this draft bill are wider than permitted under international law.

Nonetheless, the national states continue to play an important role because the physical infrastructure of the internet begins and ends in an area over which they have *de facto* and *de jure* jurisdiction. Questions about access and free and unchecked communication are therefore still concentrated within the national legal sphere. It becomes apparent

157 Richard N. Haass, *Foreign Policy Begins at Home. The Case for Putting America's House in Order*, New York: Basic Books, 2014.

in chapters III and V, which deal with issues of access, surveillance and censorship, that these are national decisions which are assessed in the light of international or regional (ECHR and EU) conventions. By contrast, section V.4 explains that the major international internet companies which play a role in internet access and the free use of the internet fall under Dutch jurisdiction only to a limited extent, namely if the acts in question are performed within that jurisdiction. In addition, there is regular discussion about when exactly this occurs in the case of internet services. The Google Spain judgment of the European Court of Justice represents a breakthrough in this respect.

The third question was to what extent businesses are responsible for protecting citizens' internet freedom in countries where they operate, and how the Dutch government, both by itself and in cooperation with other countries, can encourage businesses to assume such responsibility. This advisory report explains that the electronic communication industry is now organised very differently than in the period when the main means of communication were telephone and telex. The system of state monopolies in an international framework under public law has been replaced by a system consisting of many players. In this system, the private sector plays a major role. This has been discussed at various places in this report, particularly in chapter II and section V.4. The private sector plays an important role in the governance of the internet, and internet companies provide a variety of services such as search engines, cloud computing (sections III.4.1 and IV.3.2) and email. Sometimes they are compelled to act as extensions of the authorities, as in the case of data retention (section III.2) or censorship, which is something to which they may or may not raise objections (section V.3). The private sector therefore has considerable influence over internet freedom.

It should be noted that the position of internet companies is not always legally clear. For example, it is not clear in the Netherlands whether the social media come under telecommunication law or media law. The answer to this question has a major bearing on the extent to which they can be held liable for the content of communications and publications. Moreover, companies can find themselves backed into a corner by national jurisdictions with different legal regimes. Commercial considerations are normally decisive for internet companies, both generally and as regards the collection, processing and storage of data of internet users. As yet, it is unclear in law to what extent businesses are responsible for protecting internet freedom. This question must be viewed within the broader context of corporate social responsibility. The UN's Guiding Principles on Business and Human Rights, which have been drawn up for this purpose and are currently the subject of international consultation, are of special relevance in this area.

Recommendations

Recommendation 1
Sections III.2, III.4 and IV.3.2 explain that data of Dutch internet users are often stored on servers outside Dutch jurisdiction (cloud computing). The states where the servers are located are usually authorised to demand access to those data on certain conditions. As computers cannot process encrypted data very well, and the servers on which the data are stored are often located in jurisdictions where Dutch citizens have no legal protection, the system is potentially as leaky as a sieve. Nor do safe harbour agreements provide sufficient protection since they are ineffective, hard or impossible to enforce and contain unduly wide national security exceptions. These risks deserve the government's full attention.

The Dutch government's policy is to arrange for all dealings between government and citizen to take place online: by 2017 all government files, records and transactions must be electronic as part of the nationwide digital programme. In the AIV's opinion, it is necessary to establish as a matter of urgency whether, during storage and processing, these data may end up outside Dutch jurisdiction where they cannot be sufficiently protected, technically and legally. Policy and legislative measures must be taken to prevent such a situation, or at least to create legal safeguards to ensure that access to the data is subject to the same legal safeguards that apply in the Netherlands (see sections III.5.1 and III.5.2). Sufficient guarantees of legal protection are also important.

Recommendation 2
The Netherlands is well placed to build on its thriving internet economy. It can capitalise on this by creating a positive business climate, particularly by providing optimal protection of internet freedom in all the ways discussed in the present report. Organising international conferences and hosting international institutes have a positive spin-off, but will yield only fleeting benefits if they are not embedded in the Dutch internet community. As part of the international efforts to promote optimal internet freedom, the Netherlands could create a positive business climate for internet companies and encourage the formation of innovative internet centres staffed by specialists within the universities. Moreover, the Ministry of Economic Affairs, which plays a key role in this, should arrange for better coordination between the departments responsible for internet-related issues.

Recommendation 3
A basic aim of Dutch human rights policy and also a cornerstone of its foreign policy is to set an example (without pretending to be perfect), particularly in terms of openness and accountability: democracy and freedom in the Netherlands are the criteria. It follows that the Netherlands must also strive for the same high level of internet protection nationally as it promotes internationally. This is a responsibility of all ministries, especially those currently responsible for internet matters.

A matter deserving special consideration in relation to the pending constitutional amendment, the proposed revision of the Dutch Intelligence and Security Services Act 2002 and the draft Computer Crime III Bill is whether the policies and legislation introduced by the Netherlands are consistent with the image it wishes to convey internationally.

Recommendation 4
The need to ensure effective and independent oversight of the intelligence and security services has received huge coverage in the United States since the Snowden affair, and the subject has also been raised in the Netherlands in the course of the evaluation of the Dutch Intelligence and Security Services Act 2002, for example in a motion filed by the Christian Democratic Alliance (CDA) party in the Senate and adopted on 7 October 2014 (Senate of the States General, 2014-2015, CVIII, D). The resolution on the promotion, protection and enjoyment of human rights on the internet, which was adopted by the UN Human Rights Council in July 2012 and under which individuals have the same rights online as they have offline, should serve as the touchstone for Dutch policy. If, because of the permanent terrorist threat, measures must be taken against persons or categories of persons not suspected of any specific offence, this can be justified under the rule of law only if effective and independent oversight exists. The AIV believes that strengthening effective and independent oversight of the lawful and proportionate use of investigative and preventive measures by the Dutch Data Protection Authority and the Intelligence and Security Services Review Committee (CTIVD) is of great importance to internet freedom,

as defined in this advisory report, given the current state of the technology and the changes in international relations.

Recommendation 5
The Netherlands will spend approximately €53.5 million on human rights policy (including Radio Netherlands Worldwide) in 2014. Part of that is allocated to the promotion of internet freedom. The Netherlands is providing manpower and funding to support various important projects concerning internet freedom. However, there is no evidence that it has a coherent vision of the internet and the various aspects that must be distinguished and emphasised. Before it is decided what activities should be supported, the government should conduct a survey to identify what aspects of the problem are relevant to the Netherlands and what priorities should be set. It could, in consultation with organisations working in the field, take specific measures to promote internet freedom and security, for example by developing and publishing open source software. The failure to consider ways of improving international policy-making (the operation of the Internet Governance Forum and the reorganisation of ICANN) is regarded by the AIV as a clear omission.

Recommendation 6
Much can also be said about the Dutch role in relation to the EU's involvement in matters of internet governance. The Netherlands has adopted a wait-and-see attitude on whether or not the Safe Harbour Agreement should be renewed and on the negotiations about the Umbrella Agreement. However, the Netherlands possesses more than sufficient know-how to play a more leading role in relation to these topics. The government should take the position that unless far-reaching improvements are made to the Safe Harbour Agreement it can no longer serve as the basis for the exchange of data with the United States in the private sector. The Netherlands can use its Presidency of the EU in 2016 to make proposals to update the existing legislation relating to internet freedom.

Recommendation 7
Something which deserves special consideration is the provision of better privacy safeguards for the exchange of data between national intelligence and security services within Europe and beyond. When the Intelligence and Security Services Act 2002 is revised, the exchange of data between Dutch and foreign intelligence and security services should be regulated by law, with sufficient safeguards for the privacy of citizens, as explained in section III.2.

Recommendation 8
The activities of the private sector and internet organisations in which the internet companies play a dominant role can have a significant impact on internet freedom. Internet companies are mainly motivated by profit considerations and have to deal with divergent national and international statutory frameworks. The government's role is to monitor whether new software, protocols and the like infringe the European interpretation of the freedom of expression, privacy and data protection. NGOs can play a signalling role here.

The question of how international companies can be involved in implementing Dutch human rights policy has long been under consideration. This issue is very urgent in the context of this advisory report since just a few international companies are responsible for the transmission of information internationally (both confidential and public communications) and for the safeguards that should be provided. The government must therefore raise the issue of the responsibility of these companies in international forums and enter into a dialogue with them about human rights, just as it does with foreign governments.

Recommendation 9
As seen in numerous places in this advisory report, issues of internet freedom are not the responsibility of any single government ministry and are also increasingly connected with responsibilities that must be borne by the private sector and other stakeholders. This means that the implementation of Dutch human rights policy, particularly in this field, is a shared responsibility. The AIV therefore recommends that the formulation and preparation of policy on internet-related matters should be coordinated and constitute a shared responsibility.

Recommendation 10
The Netherlands must pursue a more consistent policy on the positions it wishes to take in the different international forums and the partners with which it wishes to form coalitions. The Ministry of Foreign Affairs must invest more money and manpower in the Internet Governance Forum. It could also advocate privacy-enhancing measures within ICANN and other internet organisations. An example was given in section V.1: the WHOIS database of the Dutch Internet Domain Registration Foundation (SIDN), which registers domain names for the .nl country code domain, does not reveal the address information of the domain name holder, other than, on request, to bailiffs and lawyers. The Netherlands could press for the adoption of such a solution internationally.

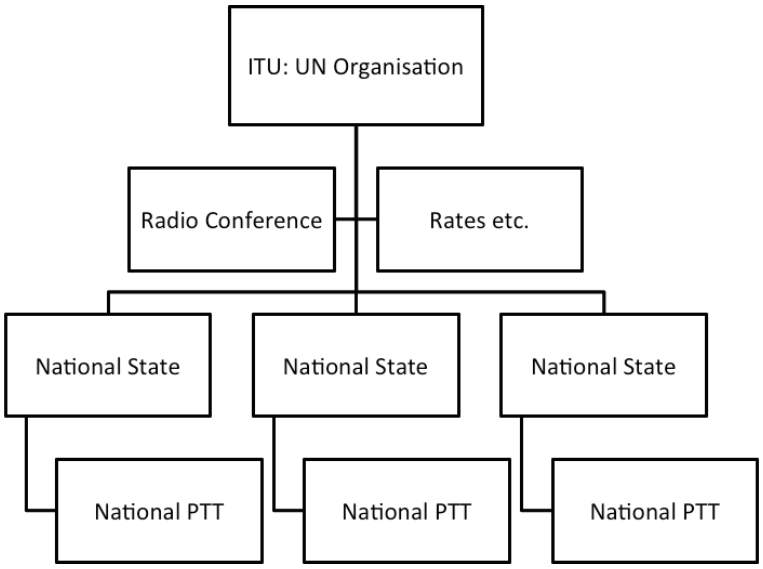
Recommendation 11
Various ministries are involved in formulating policy on internet freedom. These are the Ministry of Foreign Affairs, the Ministry of Security and Justice, the Ministry of Economic Affairs, the Ministry of the Interior and Kingdom Relations and the Ministry of Defence. The Ministry of Economic Affairs regularly consults with Dutch stakeholders in preparation for international meetings. This is an example that could be followed by other ministries. From its interviews with experts, the AIV has the impression that the Ministry of Foreign Affairs is rather out of touch with the Dutch internet community. It would be desirable for this ministry to make more personnel available to bring its knowledge of the internet, including EU-related issues, up to standard and establish closer contact with the internet community in the Netherlands and abroad.

Additional information about the history of current telecommunications

Technical infrastructure: from telephone to the internet

Section II.1 explained that international telephone traffic and the orderly use of frequencies required a stable international legal framework and consultation structure. The diagram below shows the structure of the international telecommunication sector as it then was.

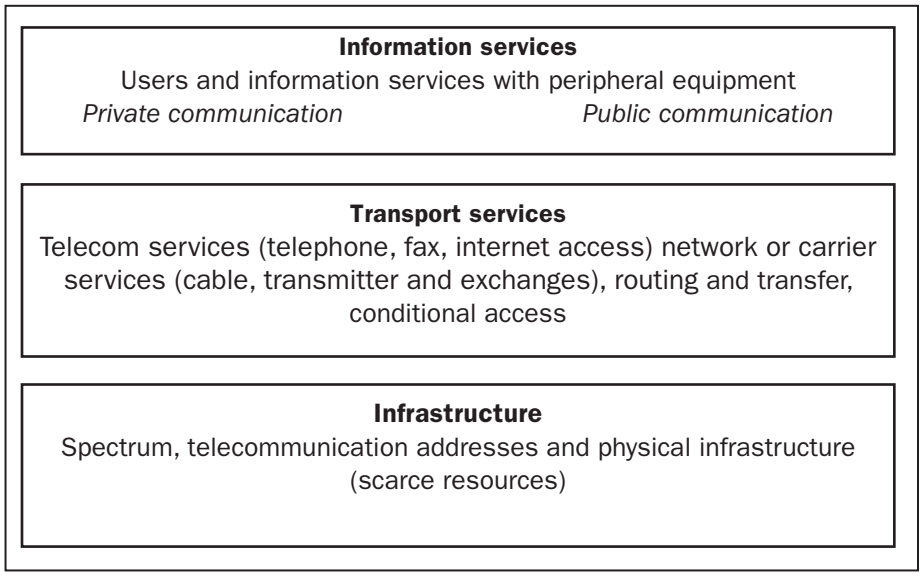
The telephony structure



Source: University of Amsterdam – Institute for Information Law

Within this organisational structure, the national PTTs developed a layered Open System Interconnection (OSI) model which provided a networking framework for the entire communication system. The lowest layer was composed of the physical infrastructure (the cables, frequencies and exchanges). Stacked on top of each other above this bottom layer were services for converting human language into machine language, for switching and routing, for security, for addressing and so forth. These services communicated with one another in accordance with fixed standards. An important feature of this model was that the human communication (content) and technical telecommunication (the data necessary for the communication to reach the right address – the traffic data) were completely segregated from one another. The PTTs were concerned solely with the traffic data. As the old Dutch saying went, 'the PTT reads the envelope, not the message'. The following diagram shows this layered model.

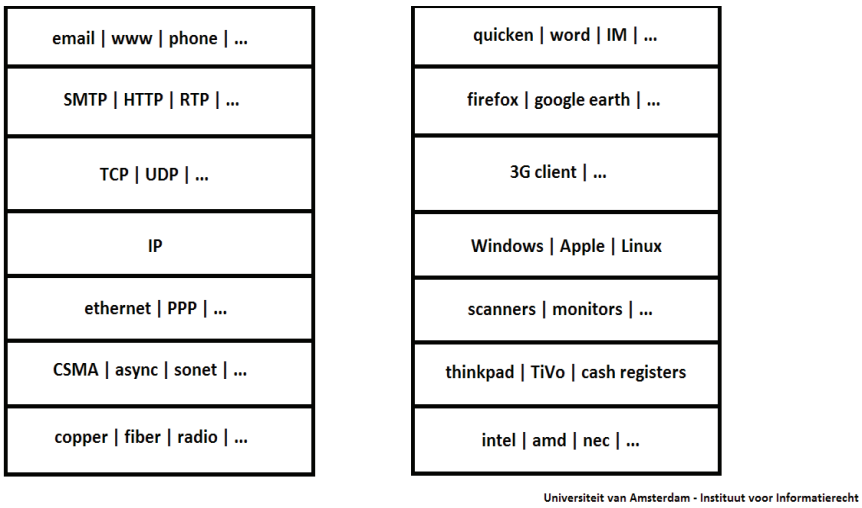
Services, transport and infrastructure



Source: University of Amsterdam - Institute for Information Law

The detachment of services and applications from the infrastructure can be represented as follows in the diagram of the model: the network on the left and the computer on the right.[158] The various abbreviations stand for the stacked protocols and software applications which work with one another on the internet and a 2014-model PC respectively. The bottom layer is the physical one. The upper layers of the applications on the PC are the layers that communicate with the internet or services that run on it.

Break-up of the layers model into telecommunications and computers



158 Source: Jonathan Zittrain, *The Future of the Internet and How to Stop It*, New Haven/London: Yale University Press, 2008, pp. 68-70.

Owing to the competition at all levels of the communication channel, the ever larger and faster bandwidths and media (fibre optics, digital frequencies and digital memory storage) and the public's changed communication pattern (switch from telephoning to sending multimedia messages), the advent of the internet at the end of the twentieth century was as great a communication revolution as that of the telephone and radio at the end of the nineteenth century. But the internet still uses the infrastructure created at that time.

The internet has a hierarchical structure similar to that of the OSI model. It too has a clear, physical layer. It differs from the OSI model in that it is harder to distinguish between content and transport. And it differs from telephony in that it is packet-switched, in other words a unique connection is not required for a communication. Moreover, it has no exchanges through which all traffic must be routed. Besides hosting a wide range of services for short messages (from email to Twitter), the internet has powerful applications (through the World Wide Web) of web browsers and search engines capable of searching the entire network and making documents, images and audio accessible worldwide (for example through Google and YouTube).

Organisations involved in the inception of the internet

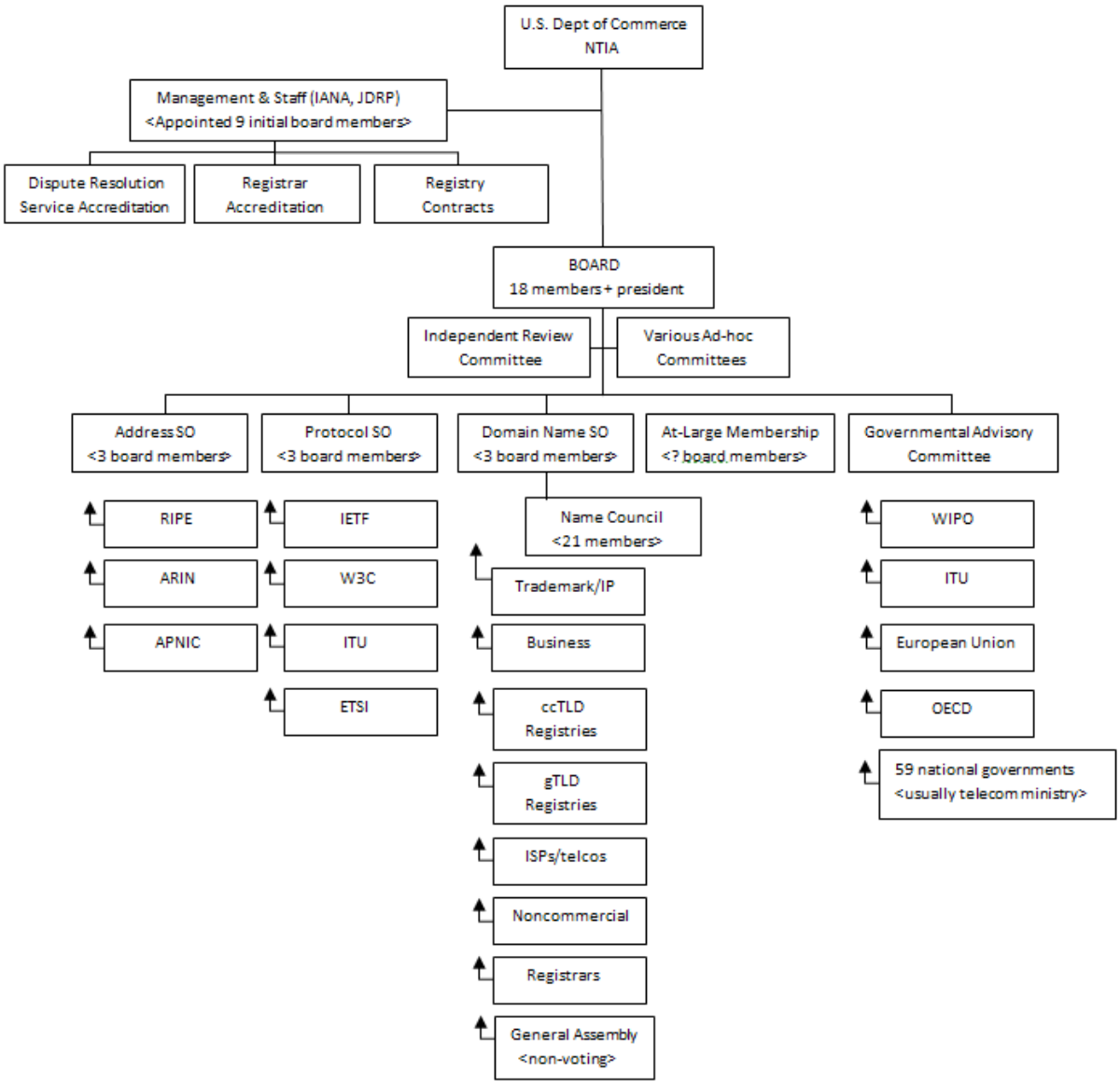
The Internet Activities Board (IAB) dates from 1983 and was the forerunner of the present Internet Architecture Board. It was the first attempt to put the governance of the internet on a formal footing. It remained closely associated with the Internet Engineering Task Force (IETF), which from the outset was an informal organisation for the discussion of open standards. It constituted a kind of anti-OSI movement. The OSI consultation bodies, which were populated by PTT engineers, were regarded as bastions of bureaucratic formalism and dominated by the principles of state control and ownership – the antithesis of the internet community's ideal of a horizontal organisation based on open standards.

The IETF still develops protocols, standards and specifications for the internet. Although it does not have any means of enforcing them, this is not necessary as the protocols, standards and specifications are still observed voluntarily (in keeping with the original ideal). Any business or individual which fails to observe them would then find it difficult, if not impossible, to gain access to the internet. Interconnectivity and shared norms and values (see Nye's analysis in chapter I) are conducive to compliance with the norm. Everyone can join in the work of the IETF. The protocols, standards and specifications are the product of consensus within working groups. The IETF is not a legal entity, but operates under the auspices of the Internet Society.

The Internet Assigned Numbers Authority (IANA) was founded in 1988. IANA worked on a contractual basis for DARPA, an agency of the US Department of Defense, which was instrumental in the development of the internet. This contract more or less designated Jon Postel, a key figure in the development of the internet, as the authority ('the IANA'). IANA concerned itself with the development of the IP addresses and related activities. Here too the picture was one of autonomous development. Milton Mueller describes this as follows:[159] 'Explicit claims on the right to manage name and address assignment were being made by an authority (…) that lacked any basis in formal law or state action. The authority claims nevertheless had significant legitimacy within the technical community.'

159 Milton Mueller, *Ruling the Root*, Massachusetts: Massachusetts Institute for Technology, 2002, p. 93.

The diagram below shows ICANN's organisational structure at the time of its establishment.[160] Under ICANN's board are various advisory bodies: the Address Supporting Organization, the Protocol Supporting Organization, the Domain Name Supporting Organization, the At-Large Membership and the Governmental Advisory Committee. These advisory bodies consist of representatives of the organisations shown in the column below each of the bodies. One of the functions of the supporting organisations is to foster consensus within the part of the internet community they represent.



160 Idem, p. 173, figure 8.1.

In brief, this is about addresses (far left column), protocols and standards (second column from left) and names (middle column). The far right column represents the old stakeholders and state interests. The second column from the right (At-Large Membership) is for NGOs which do not belong in the other columns. The diagram does not include ISOC, although it maintains links with other organisations included in the diagram. The Protocol Supporting Organization, the body responsible for technical standards (second column from the left), has now been disbanded. ICANN is the spider in the web. The US Department of Commerce oversees this collection of old and new representatives of world telecommunications through the National Telecommunications and Information Administration.

Consultations have been going on for years in these organisations about the transition from IPv4 numbers to the longer IPv6 numbers, given the looming scarcity of the former. The new numbers are gradually being introduced. The main policy debate within ICANN is about the introduction and assignment of new generic top-level domains (gTLDs). A fairly heated discussion is taking place between stakeholders with an interest in trademarks and geographical names about the introduction of generic names (e.g. new gTLDs such as '.wine', '.amazon' and '.patagonia'). Tendering procedures are now under way for the new domains.

ICANN has a Joint Project Agreement and a contract with the US Department of Commerce for the assignment of the internet addresses and the management of gTLDs. Under this contract ICANN has the following tasks:

- establish policy for the allocation of IP number blocks;
- oversight of the root server system;
- oversight of the policy for adding new top-level domains to the root system;
- coordination of the assignment of other technical parameters to maintain universal connectivity on the internet;
- other activities necessary to coordinate the specified DNS management functions, as agreed between the Department of Commerce and ICANN.

The Joint Project Agreement has been repeatedly extended and amended. In the process, ICANN's autonomy has been gradually increased, although the Department of Commerce continues to have an oversight role.[161] In the Affirmation of Commitments between the Department and ICANN of 30 September 2009 the Joint Project Agreement was extended for an indefinite term.[162] The National Telecommunications and Information Administration of the Department of Commerce has evolved into a kind of process monitor. Although all parties have been able to live with this, the link between ICANN and the United States has become untenable in the wake of the Snowden affair.

ICANN is managed by a board of directors, whose members represent a number of groups. The board has 20 members, 16 of whom have voting rights. Half of those entitled to vote are nominated to the board by the Nominating Committee. The others are elected by the constituent organs of ICANN, including the Country Code

161 Lee A. Bygrave and others, 'The naming game: governance of the domain name system', in: Lee. A. Bygrave and Jon Bing, *Internet Governance, Infrastructure and Institutions*, Oxford: Oxford University Press, 2009, pp. 151-153.

162 See: <http://www.ntia.doc.gov/page/docicann-agreements>, consulted on 5 June 2014.

Names Supporting Organization (membership of which is open to organisations that manage country-specific top-level domains), the Generic Names Supporting Organization (membership of which is open to organisations that manage generic top-level domains) and the at-large members. The board also has five advisory members, including representatives of the Governmental Advisory Committee (membership open to every state) and the Internet Engineering Task Force. The Nominating Committee too consists of representatives of various constituencies and stakeholder groups. Another requirement is that the board of directors must reflect cultural and geographic diversity.[163] However, the existence of many cross-links between these organisations and bodies means that the structure of ICANN is opaque. For example, some of the organisations that are members of the board are also represented on the Nominating Committee. ICANN's revenues include the annual payments for the use of top-level domains. This is a substantial sum as 125 million .com domain names have already been registered and there will be many more generic top-level domains. Although ICANN's financial affairs are subject to strict internal control rules, its Chief Executive Officer has fairly far-reaching discretionary powers to donate funds to good causes and so forth. This is in keeping with the legal form of ICANN, namely that of a non-profit public benefit corporation under the law of California.

The Working Group on Internet Governance (WGIG) succeeded in formulating a working definition of internet governance (see section V.1), but remained vague about the scope of the term. It also identified policy issues relevant to internet governance, but did not manage to make substantive recommendations. It noted that there was no international forum in which the identified issues could be discussed and therefore recommended the establishment of a global multistakeholder forum. As the WGIG was unable to reach agreement about the institutional arrangements for internet governance, its report made proposals for four governance models. One of the elements was ICANN's role. One of the models envisaged that ICANN would fall under a UN organisation. The WGIG also recommended that no government whatever should have a privileged role in internet governance, which was a direct attack on the dominant position of the United States in the management of domain names.

163 See: <https://www.icann.org/resources/pages/bylaws-2012-02-25-en#/II>, consulted on 5 June 2014.

Annexe IIa

Request for advice

Mr J.G. de Hoop Scheffer
Chairman of the Advisory Council
on International Affairs
P.O. Box 20061
2500 EB The Hague

Date 20 February 2014
Re Request for advice on internet freedom

Dear Mr De Hoop Scheffer,

'Internet freedom' is a major priority of Dutch human rights foreign policy. The basic principle of internet freedom is that fundamental rights offline should also apply online. The rights to privacy, data protection, confidential communications and freedom of expression are particularly notable examples.[1] The recent UN resolution on the right to privacy in the digital age, which was cosponsored by the Netherlands, articulates this principle clearly.[2] To reinforce the principle, the Netherlands is developing initiatives on its own and with other countries. Two years ago, for instance, the Netherlands established the Freedom Online Coalition (FOC). The FOC now numbers 22 countries and is dedicated to promoting internet freedom across the globe. The coalition organises a multistakeholder conference each year and provides financial assistance to bloggers and cyber activists under threat through the Digital Defenders Partnership.

The FOC, and also the International Conference on Cyberspace, which will be held in the Netherlands in 2015, demonstrate that the Netherlands is an international leader when it comes to internet freedom. A growing number of countries, however, want to exert more control over the internet (and its infrastructure) and are developing initiatives to that end. Governments around the world, including the Dutch government, also face the challenge of striking a good balance between freedom and security in different contexts, while respecting citizens' privacy rights. These trends are putting pressure on internet freedom.

The recent revelations surrounding the US National Security Agency (NSA) have brought the debate on security and internet freedom to a head. One issue is how rights which apply online can be embedded as effectively as possible in national and international legislation and policy. This discussion is being guided by, *inter alia*, the above-mentioned UN resolution on the right to privacy. In addition, the 'Necessary and Proportionate' principles[3] may serve as inspiration.[4] This document, which was drawn up on the initiative of civil society

1 See articles 10, 13 and 7 of the Dutch Constitution, articles 8 and 10 of the European Convention on Human Rights (ECHR) and articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR).
2 Resolution by the General Assembly of the United Nations of 1 November 2013 (A/C.3/68/L.45).
3 Other examples include the ECHR and resolutions by the Council of Europe.
4 The ECHR and resolutions by the Council of Europe can similarly provide guidance.

organisations, sets forth the 13 principles which, in the initiators' view, ought to apply to modern types of surveillance.[5]

An advisory report by the Advisory Council on International Affairs (AIV) could fuel and illuminate the debate, which, as is well known, is also being conducted intensely in the Netherlands.

The government would therefore like to present the following questions to the AIV:

1. How can the Dutch government ensure that internet freedom[6] is embedded and further operationalised in Dutch domestic and foreign policy as effectively as possible, against the background of:

a) the challenge facing governments, including the Dutch government, in weighing the right to privacy – as formulated in the UN resolution on this right[7] – against other interests to be protected by those governments as they look for solutions to issues raised by digital communications;
b) the leading role of the Netherlands in foreign policy concerning internet freedom, as illustrated by the FOC, and the opportunities which the Netherlands has to influence the international debate, including the International Conference on Cyberspace in the spring of 2015;
c) an international playing field in which more and more countries are seeking to exert tighter control over the internet (and its infrastructure) and are developing initiatives to that end;
d) the right to protection of personal data, which is addressed in different ways by the UN, the Council of Europe and the EU.

2. Is Dutch jurisdiction over internet freedom limited to activities in the Netherlands, or does it, by virtue of the increased technological possibilities, extend to situations outside the country?[8] If such jurisdiction does not extend this far, how can the Dutch government help to effectively safeguard internet freedom beyond the Netherlands' borders?

3. To what extent are businesses responsible for protecting citizens' internet freedom in countries where they operate, and how can the Dutch government, both by itself and in cooperation with other countries, encourage businesses to assume such responsibility?[9]

I look forward to receiving your advisory report.

Yours sincerely,

Frans Timmermans
Minister of Foreign Affairs

5 See: <https://necessaryandproportionate.org/text>. These principles have been endorsed by more than 350 organisations and more than 50 independent experts throughout the world. Sweden has also embraced seven of the principles <https://www.privacyinternational.org/blog/swedens-foreign-minister-declares-his-support-for-principles to-protect-privacy-in-the-face-of>.
6 See footnote 1.
7 See footnote 2.
8 See preamble, tenth paragraph, of the UN resolution mentioned in footnote 2.
9 For example, through the Freedom Online Coalition and the Council of Europe.

United Nations A/C.3/68/L.45

General Assembly

Distr.: Limited
1 November 2013

Original: English

Sixty-eighth session
Third Committee
Agenda item 69 (b)
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Brazil and Germany: draft resolution

The right to privacy in the digital age

The General Assembly,

Reaffirming the purposes and principles of the Charter of the United Nations,

Reaffirming also the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights,

Reaffirming further the Vienna Declaration and Programme of Action,

Noting that the rapid pace of technological development enables individuals in all regions to use new information and communication technologies and at the same time enhances the capacity of Governments, companies and individuals for surveillance, interception and data collection, which may violate human rights, in particular the right to privacy, as enshrined in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,

Reaffirming the human right of individuals to privacy and not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, and the right to enjoy protection of the law against such interferences and attacks, and recognizing that the exercise of the right to privacy is an essential requirement for the realization of the right to freedom of expression and to hold opinions without interference, and one of the foundations of a democratic society,

Stressing the importance of the full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation,

13-54407 (E) 051113

Welcoming the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,[1] submitted to the Human Rights Council at its twenty-third session, concerning the implications of States' surveillance of communications and the interception of personal data for the exercise of the human right to privacy,

Emphasizing that illegal surveillance of communications, their interception and the illegal collection of personal data constitute a highly intrusive act that violates the right to privacy and freedom of expression and may threaten the foundations of a democratic society,

Noting that while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law,

Deeply concerned at human rights violations and abuses that may result from the conduct of any surveillance of communications, including extraterritorial surveillance of communications, their interception and the collection of personal data, in particular massive surveillance, interception and data collection,

Recalling that States must ensure that measures taken to counter terrorism comply with international law, in particular international human rights, refugee and humanitarian law,

1. *Reaffirms* the rights contained in the International Covenant on Civil and Political Rights, in particular the right to privacy and not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, and the right to enjoy protection of the law against such interference or attacks, in accordance with article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights;

2. *Recognizes* the rapid advancement in information and communications technologies, including the global and open nature of the Internet, as a driving force in accelerating progress towards development in its various forms;

3. *Affirms* that the same rights that people have offline must also be protected online, in particular the right to privacy;

4. *Calls upon* all States:

(a) To respect and protect the rights referred to in paragraph 1 above, including in the context of digital communication;

(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection, with a view to upholding the right to privacy and ensuring the full and effective implementation of all their obligations under international human rights law;

[1] A/HRC/23/40 and Corr.1.

(d) To establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data;

5. *Requests* the United Nations High Commissioner for Human Rights to submit an interim report on the protection of the right to privacy in the context of domestic and extraterritorial surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection of personal data, to the General Assembly at its sixty-ninth session, and a final report at its seventieth session, with views and recommendations, to be considered by Member States, with the purpose of identifying and clarifying principles, standards and best practices on how to address security concerns in a manner consistent with States' obligations under international human rights law and with full respect for human rights, in particular with respect to surveillance of digital communications and the use of other intelligence technologies that may violate the human right to privacy and freedom of expression and of opinion;

6. *Decides* to examine the question on a priority basis at its sixty-ninth session, under the sub-item entitled "Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms" of the item entitled "Promotion and protection of human rights".

International Principles on the Application of Human Rights to Communications Surveillance

FINAL VERSION 10 JULY 2013

As technologies that facilitate State surveillance of communications advance, States are failing to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. This document attempts to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. These principles can provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

Preamble

Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognised under international human rights law.[1] Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[2]

Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to State communications surveillance. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. The explosion of digital communications content and information about communications, or "communications metadata" – information about an individual's communications or use of electronic devices – the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make State surveillance possible at an unprecedented scale.[3] Meanwhile, conceptualisations of existing human rights law have not kept up with the modern and changing communications surveillance capabilities of the State, the ability of the State to combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.

The frequency with which States are seeking access to both communications content and communications metadata is rising dramatically, without adequate scrutiny.[4] When accessed and analysed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications.[5] Despite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, legislative and policy instruments often afford communications metadata a lower level of protection and do not place sufficient restrictions on how they can be subsequently used by agencies, including how they are data-mined, shared, and retained.

In order for States to actually meet their international human rights obligations in relation to communications surveillance, they must comply with the principles set out below. These principles apply to surveillance conducted within a State or extraterritorially. The principles also apply regardless of the purpose for the surveillance – law enforcement, national security or any other regulatory purpose. They also apply both to the State's obligation to respect and fulfil individuals' rights, and also to the obligation to protect individuals' rights from abuse by non-State actors, including corporate entities.[6] The private sector bears equal responsibility for respecting human rights, particularly given the key role it plays in designing, developing and disseminating technologies; enabling and providing communications; and - where required - cooperating with State surveillance activities. Nevertheless, the scope of the present Principles is limited to the obligations of the State.

Changing technology and definitions

"Communications surveillance" in the modern environment encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future. "Communications" include activities, interactions and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

Traditionally, the invasiveness of communications surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content", "subscriber information" or "metadata", stored data or in transit data, data held in the home or in the possession of a third party service provider.[7] However, these distinctions are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time,[8] or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law.

In evaluating the invasiveness of State communications surveillance, it is necessary to consider both the potential of the surveillance to reveal protected information, as well as the purpose for which the information is sought by the State. Communications surveillance that will likely lead to the revelation of protected information that may place a person at risk of investigation, discrimination or violation of human rights will constitute a serious infringement on an individual's right to privacy, and will also undermine the enjoyment of other fundamental rights, including the right to free expression, association, and political participation. This is because these rights require people to be able to communicate free from the chilling effect of government surveillance. A determination of both the character and potential uses of the information sought will thus be necessary in each specific case.

When adopting a new communications surveillance technique or expanding the scope of an existing technique, the State should ascertain whether the information likely to be procured falls within the ambit of "protected information" before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism. In considering whether information obtained through communications surveillance rises to the level of "protected information", the form as well as the scope and duration of the surveillance are relevant factors. Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection.[9]

The determination of whether the State may conduct communications surveillance that interferes with protected information must be consistent with the following principles.

The Principles

LEGALITY: Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

LEGITIMATE AIM: Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

NECESSITY: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

ADEQUACY: Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

PROPORTIONALITY: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.

Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

1. there is a high degree of probability that a serious crime has been or will be committed;
2. evidence of such a crime would be obtained by accessing the protected information sought;
3. other available less invasive investigative techniques have been exhausted;

4. information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and
5. information is accessed only by the specified authority and used for the purpose for which authorisation was given.

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

1. other available less invasive investigative techniques have been considered;
2. information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
3. information is accessed only by the specified authority and used for the purpose for which was authorisation was given.

COMPETENT JUDICIAL AUTHORITY: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. separate from the authorities conducting communications surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and
3. have adequate resources in exercising the functions assigned to them.

DUE PROCESS: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,[10] except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

USER NOTIFICATION: Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstances:

1. Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or
2. Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; and
3. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

TRANSPARENCY: States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

PUBLIC OVERSIGHT: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.[11] Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.[12]

SAFEGUARDS FOR INTERNATIONAL COOPERATION: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS: States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

[1] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[2] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[3] Communications metadata may include information about our identities (subscriber information, device information), interactions (origins and destinations of communications, especially those showing websites visited, books and other materials read, people interacted with, friends, family, acquaintances, searches conducted, resources used), and location (places and times, proximities to others); in sum, metadata provides a window into nearly every action in modern life, our mental states, interests, intentions, and our innermost thoughts.

[4] For example, in the United Kingdom alone, there are now approximately 500,000 requests for communications metadata every year, currently under a self-authorising regime for law enforcement agencies who are able to authorise their own requests for access to information held by service providers. Meanwhile, data provided by Google's Transparency reports shows that requests for user data from the U.S. alone rose from 8888 in 2010 to 12,271 in 2011. In Korea, there were about 6 million subscriber/poster information requests every year and about 30 million requests for other forms of communications metadata every year in 2011-2012, almost of all of which were granted and executed. 2012 data available at <http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586>.

[5] See as examples, a review of Sandy Petland's work, 'Reality Mining', in MIT's Technology Review, 2008, available at <http://www2.technologyreview.com/article/409598/tr10-reality-mining/> and also see Alberto Escudero-Pascual and Gus Hosein, 'Questioning lawful access to traffic data', Communications of the ACM, Volume 47 Issue 3, March 2004, pages 77-82.

[6] Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 16 2011, available at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf>.

[7] "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[8] "Short-term monitoring of a person's movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." United States v. Jones, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

[9] "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.) p. 562; U.S. v. Jones, 565 U.S. __, (2012), Alito, J., concurring. "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paras. 43-44.

[10] The term "due process" can be used interchangeably with "procedural fairness" and "natural justice", and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

[11] The UK Interception of Communications Commissioner is an example of such an independent oversight mechanism. The ICO publishes a report that includes some aggregate data but it does not provide sufficient data to scrutinise the types of requests, the extent of each access request, the purpose of the requests, and the scrutiny applied to them. See <http://www.iocco-uk.info/sections.asp?sectionID=2&type=top>.

[12] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para 84.

List of abbreviations

AIV	Advisory Council on International Affairs
AIVD	General Intelligence and Security Service
CJEU	Court of Justice of the European Union
CTIVD	Intelligence and Security Services Review Committee
DNS	Domain Name System
DTP	Datafile Transfer Protocol
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EU	European Union
FISC	Foreign Intelligence Surveillance Court
FTC	Federal Trade Commission
GAC	Governmental Advisory Committee
gTLD	generic top-level domain
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communication technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet Protocol
ISOC	Internet Society
ITR	International Telecommunications Regulations
ITU	International Telecommunication Union
NGO	non-governmental organisation
NSA	National Security Agency
OSI	Open System Interconnection
PCLOB	Privacy & Civil Liberties Oversight Board
PTT	post, telegraph and telephone
SIDN	Internet Domain Registration Foundation
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIA	Total Information Awareness

TCP	Transmission Control Protocol
TFTP	Terrorist Finance Tracking Program
UN	United Nations
US	United States
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WIV	Intelligence and Security Services Act
WODC	Research and Documentation Centre
WSIS	World Summit on the Information Society
WWW	World Wide Web

List of persons consulted

Name	Position/organisation
Caspar Bowden	Independent privacy researcher
Dr Quirine Eijkman	Head of Political Affairs & Press Office at Amnesty International Dutch Section
Hielke Hijmans	Head of Policy & Consultation Unit at the European Data Protection Supervisor (on sabbatical leave)
Professor Erik Huizer	CTO at SURFnet and professor of internet applications at Utrecht University
Professor Milton Mueller	Syracuse University School of Information Studies, Syracuse, New York, United States
Rejo Zenger	Researcher, Bits of Freedom
Hans de Zwart	Director, Bits of Freedom

Previous reports published by the Advisory Council on International Affairs

1 AN INCLUSIVE EUROPE, *October 1997*
2 CONVENTIONAL ARMS CONTROL: urgent need, limited opportunities, *April 1998*
3 CAPITAL PUNISHMENT AND HUMAN RIGHTS: recent developments, *April 1998*
4 UNIVERSALITY OF HUMAN RIGHTS AND CULTURAL DIVERSITY, *June 1998*
5 AN INCLUSIVE EUROPE II, *November 1998*
6 HUMANITARIAN AID: redefining the limits, *November 1998*
7 COMMENTS ON THE CRITERIA FOR STRUCTURAL BILATERAL AID, *November 1998*
8 ASYLUM INFORMATION AND THE EUROPEAN UNION, *July 1999*
9 TOWARDS CALMER WATERS: a report on relations between Turkey and the European Union, *July 1999*
10 DEVELOPMENTS IN THE INTERNATIONAL SECURITY SITUATION IN THE 1990s: from unsafe security to unsecured safety, *September 1999*
11 THE FUNCTIONING OF THE UNITED NATIONS COMMISSION ON HUMAN RIGHTS, *September 1999*
12 THE IGC AND BEYOND: TOWARDS A EUROPEAN UNION OF THIRTY MEMBER STATES, *January 2000*
13 HUMANITARIAN INTERVENTION, *April 2000**
14 KEY LESSONS FROM THE FINANCIAL CRISES OF 1997 AND 1998, *April 2000*
15 A EUROPEAN CHARTER OF FUNDAMENTAL RIGHTS?, *May 2000*
16 DEFENCE RESEARCH AND PARLIAMENTARY SCRUTINY, *December 2000*
17 AFRICA'S STRUGGLE: security, stability and development, *January 2001*
18 VIOLENCE AGAINST WOMEN: LEGAL DEVELOPMENTS, *February 2001*
19 A MULTI-TIERED EUROPE: the relationship between the European Union and subnational authorities, *May 2001*
20 EUROPEAN MILITARY-INDUSTRIAL COOPERATION, *May 2001*
21 REGISTRATION OF COMMUNITIES BASED ON RELIGION OR BELIEF, *June 2001*
22 THE WORLD CONFERENCE AGAINST RACISM AND THE RIGHT TO REPARATION, *June 2001*
23 COMMENTARY ON THE 2001 MEMORANDUM ON HUMAN RIGHTS POLICY, *September 2001*
24 A CONVENTION, OR CONVENTIONAL PREPARATIONS? The European Union and the ICG 2004, *November 2001*
25 INTEGRATION OF GENDER EQUALITY: a matter of responsibility, commitment and quality, *January 2002*
26 THE NETHERLANDS AND THE ORGANISATION FOR SECURITY AND COOPERATION IN EUROPE IN 2003: role and direction, *May 2002*
27 BRIDGING THE GAP BETWEEN CITIZENS AND BRUSSELS: towards greater legitimacy and effectiveness for the European Union, *May 2002*
28 AN ANALYSIS OF THE US MISSILE DEFENCE PLANS: pros and cons of striving for invulnerability, *August 2002*
29 PRO-POOR GROWTH IN THE BILATERAL PARTNER COUNTRIES IN SUB-SAHARAN AFRICA: an analysis of poverty reduction strategies, *January 2003*
30 A HUMAN RIGHTS BASED APPROACH TO DEVELOPMENT COOPERATION, *April 2003*
31 MILITARY COOPERATION IN EUROPE: possibilities and limitations, *April 2003*
32 BRIDGING THE GAP BETWEEN CITIZENS AND BRUSSELS: towards greater legitimacy and effectiveness for the European Union, *April 2003*
33 THE COUNCIL OF EUROPE: less can be more, *October 2003*
34 THE NETHERLANDS AND CRISIS MANAGEMENT: three issues of current interest, *March 2004*

35 FAILING STATES: a global responsibility, *May 2004**
36 PRE-EMPTIVE ACTION, *July 2004**
37 TURKEY: towards membership of the European Union, *July 2004*
38 THE UNITED NATIONS AND HUMAN RIGHTS, *September 2004*
39 SERVICES LIBERALISATION AND DEVELOPING COUNTRIES: does liberalisation produce deprivation?, *September 2004*
40 THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE, *February 2005*
41 REFORMING THE UNITED NATIONS: A closer look at the Annan report, *May 2005*
42 THE INFLUENCE OF CULTURE AND RELIGION ON DEVELOPMENT: Stimulus or stagnation?, *June 2005*
43 MIGRATION AND DEVELOPMENT COOPERATION: coherence between two policy areas, *June 2005*
44 THE EUROPEAN UNION'S NEW EASTERN NEIGHBOURS, *July 2005*
45 THE NETHERLANDS IN A CHANGING EU, NATO AND UN, *July 2005*
46 ENERGISED FOREIGN POLICY: security of energy supply as a new key objective, *December 2005***
47 THE NUCLEAR NON-PROLIFERATION REGIME: The importance of an integrated and multilateral approach, *January 2006*
48 SOCIETY AND THE ARMED FORCES, *April 2006*
49 COUNTERTERRORISM FROM AN INTERNATIONAL AND EUROPEAN PERSPECTIVE, *September 2006*
50 PRIVATE SECTOR DEVELOPMENT AND POVERTY REDUCTION, *October 2006*
51 THE ROLE OF NGOS AND THE PRIVATE SECTOR IN INTERNATIONAL RELATIONS, *October 2006*
52 EUROPE A PRIORITY!, *November 2006*
53 THE BENELUX: the benefits and necessity of enchanced cooperation, *February 2007*
54 THE OECD OF THE FUTURE, *March 2007*
55 CHINA IN THE BALANCE: towards a mature relationship, *April 2007*
56 DEPLOYMENT OF THE ARMED FORCES: interaction between national and international decision-making, *May 2007*
57 THE UN HUMAN RIGHTS TREATY SYSTEM: strengthening the system step by step in a politically charged context, *July 2007*
58 THE FINANCES OF THE EUROPEAN UNION, *December 2007*
59 EMPLOYING PRIVATE MILITARY COMPANIES: a question of responsibility, *December 2007*
60 THE NETHERLANDS AND EUROPEAN DEVELOPMENT POLICY, *May 2008*
61 COOPERATION BETWEEN THE EUROPEAN UNION AND RUSSIA: a matter of mutual interest, *July 2008*
62 CLIMATE, ENERGY AND POVERTY REDUCTION, *November 2008*
63 UNIVERSALITY OF HUMAN RIGHTS: principles, practice and prospects, *November 2008*
64 CRISIS MANAGEMENT OPERATIONS IN FRAGILE STATES: the need for a coherent approach, *March 2009*
65 TRANSITIONAL JUSTICE: justice and peace in situations of transition, *April 2009**
66 DEMOGRAPHIC CHANGES AND DEVELOPMENT COOPERATION, *July 2009*
67 NATO'S NEW STRATEGIC CONCEPT, *January 2010*
68 THE EU AND THE CRISIS: lessons learned, *January 2010*
69 COHESION IN INTERNATIONAL COOPERATION: Response to the WRR (Advisory Council on Government Policy) Report '*Less Pretension, More Ambition', July 2010*
70 THE NETHERLANDS AND THE RESPONSIBILITY TO PROTECT: the responsibility to protect people from mass atrocities, *June 2010*
71 THE EU'S CAPACITY FOR FURTHER ENLARGEMENT, *July 2010*
72 COMBATING PIRACY AT SEA: a reassessment of public and private responsibilities, *December 2010*
73 THE HUMAN RIGHTS OF THE DUTCH GOVERNMENT: identifying constants in a changing world, *February 2011*

74 THE POST-2015 DEVELOPMENT AGENDA: the millennium development goals in perspective, *April 2011*
75 REFORMS IN THE ARAB REGION: prospects for democracy and the rule of law?, *May 2011*
76 THE HUMAN RIGHTS POLICY OF THE EUROPEAN UNION: between ambition and ambivalence, *July 2011*
77 CYBER WARFARE*, December 2011**
78 EUROPEAN DEFENCE COOPERATION: sovereignty and the capacity to act*, January 2012*
79 THE ARAB REGION, AN UNCERTAIN FUTURE, *May 2012*
80 UNEQUAL WORLDS: poverty, growth, inequality and the role of international cooperation, *September 2012*
81 THE NETHERLANDS AND THE EUROPEAN PARLIAMENT: investing in a new relationship, *November 2012*
82 INTERACTION BETWEEN ACTORS IN INTERNATIONAL COOPERATION: towards flexibility and trust, *February 2013*
83 BETWEEN WORDS AND DEEDS: prospects for a sustainable peace in the Middle East, *March 2013*
84 NEW PATHS TO INTERNATIONAL ENVIRONMENTAL COOPERATION, *March 2013*
85 CRIME, CORRUPTION AND INSTABILITY: an exploratory report, *May 2013*
86 ASIA ON THE RISE: strategic significance and implications, *December 2013*
87 THE RULE OF LAW: safeguard for European citizens and foundation for European cooperation, *January 2014*
88 PUBLIC SUPPORT FOR THE EUROPEAN UNION: building trust, *April 2014*
89 IMPROVING GLOBAL FINANCIAL COHESION: the Importance of a Coherent International Economic and Financial Architecture, *June 2014*
90 THE FUTURE OF THE ARCTIC REGION: cooperation or confrontation?, *September 2014*
91 THE NETHERLANDS AND THE ARAB REGION: a principled and pragmatic approach, *November 2014*

Advisory letters issued by the Advisory Council on International Affairs

1 Advisory letter THE ENLARGEMENT OF THE EUROPEAN UNION, *December 1997*
2 Advisory letter THE UN COMMITTEE AGAINST TORTURE, *July 1999*
3 Advisory letter THE CHARTER OF FUNDAMENTAL RIGHTS, *November 2000*
4 Advisory letter ON THE FUTURE OF THE EUROPEAN UNION, *November 2001*
5 Advisory letter THE DUTCH PRESIDENCY OF THE EU IN 2004, *May 2003****
6 Advisory letter THE RESULTS OF THE CONVENTION ON THE FUTURE OF EUROPE, *August 2003*
7 Advisory letter FROM INTERNAL TO EXTERNAL BORDERS. Recommendations for developing a common European asylum and immigration policy by 2009, *March 2004*
8 Advisory letter THE DRAFT DECLARATION ON THE RIGHTS OF INDIGENOUS PEOPLES: from Deadlock to Breakthrough?, *September 2004*
9 Advisory letter OBSERVATIONS ON THE SACHS REPORT: How do we attain the Millennium Development Goals?, *April 2005*
10 Advisory letter THE EUROPEAN UNION AND ITS RELATIONS WITH THE DUTCH CITIZENS, *December 2005*
11 Advisory letter COUNTERTERRORISM IN A EUROPEAN AND INTERNATIONAL PERSPECTIVE: interim report on the prohibition of torture, *December 2005*
12 Advisory letter RESPONSE TO THE 2007 HUMAN RIGHTS STRATEGY, *November 2007*
13 Advisory letter AN OMBUDSMAN FOR DEVELOPMENT COOPERATION, *December 2007*

14 Advisory letter CLIMATE CHANGE AND SECURITY, *January 2009*
15 Advisory letter THE EASTERN PARTNERSHIP, *February 2009*
16 Advisory letter DEVELOPMENT COOPERATION, The benefit of and need for public support, *May 2009*
17 Advisory letter OPEN LETTER TO A NEW DUTCH GOVERNMENT, *June 2010*
18 Advisory letter THE EUROPEAN COURT OF HUMAN RIGHTS: Protector of civil rights and liberties, *November 2011*
19 Advisory letter TOWARDS ENHANCED ECONOMIC AND FINANCIAL GOVERNANCE IN THE EU, *February 2012*
20 Advisory letter IRAN'S NUCLEAR PROGRAMME: Towards de-escalation of a nuclear crisis, *April 2012*
21 Advisory letter THE RECEPTOR APPROACH: A question of weight and measure, *April 2012*
22 Advisory letter OPEN LETTER TO A NEW DUTCH GOVERNMENT: The armed forces at risk, *September 2012*
23 Advisory letter TOWARDS A STRONGER SOCIAL DIMENSION OF THE EUROPEAN UNION, *June 2013*
24 Advisory letter FULL SPEED AHEAD: Response by the Advisory Council on International Affairs to the policy letter 'Respect and Justice for All', *September 2013*
25 Advisory letter DEVELOPMENT COOPERATION: Beyond a Definition, *May 2014*
26 Advisory letter THE EU'S DEPENDENCE ON RUSSIAN GAS: How an integrated EU policy can reduce it, *June 2014*

* Issued jointly by the Advisory Council on International Affairs (AIV) and the Advisory Committee on Issues of Public International Law (CAVV).

** Joint report by the Advisory Council on International Affairs (AIV) and the General Energy Council.

*** Joint report by the Advisory Council on International Affairs (AIV) and the Advisory Committee on Aliens Affairs (ACVZ).