The EU regulatory framework for the internet

Iglesias Portela, Maria José; VALCKE, Peggy; DIMITROV, George; LIEVENS, EVA; PARILLI, DAVIDE M.; STEVENS, DAVID; VAN EMELEN, TIM; VERGOTE, PETER; WERKERS, EVI

Published in:
Telecommunications, broadcasting and the internet EU competition law & regulation

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

Chapter III

The EU Regulatory Framework for the Internet

Peggy Valcke, George Dimitrov, Maria Iglesias, Eva Lievens, Davide M. Parilli, David Stevens, Tim van Emelen, Peter Vergote and Evi Werkers

A. Introduction

3–001 What is the internet?—The internet is generally described as a "network of networks".[1] In fact, it consists of a global network interconnecting computers around the world, through the use of an open protocol, the Internet Protocol (IP).[2] The internet was initially developed at the end of the 1960s by the US military. It was subsequently adopted by universities in the 1970s and 1980s as a means to link the scientific community together and to provide easy and speedy access to information resources. It was only during the second half of the 1990s that commercial use of the internet developed, as private businesses perceived its potential benefits. The use of an open protocol such as IP allows the interoperability of various types of networks and facilities (*e.g.* copper and fibre optic circuits, coaxial cable and wireless connections) and the provision of various types of services over the same network. The internet is a decentralised network without any central point of control or access, with the result that any "host" computer (*i.e.* server) can be accessed from any connected computer anywhere in the world. The internet is also a packet-switched network, which means that messages are broken down into small packets of data, each of which is transmitted separately through the system. Each data packet bears routing information enabling the transmission equipment (*i.e.* the router) through which it passes to know to which computer it should be sent. The data packets are reassembled in the correct order upon arrival at their intended destination (another computer), so that the message can be read by the computer user. Packet-switched networks must be distinguished from circuit-switched networks, such as the public switched telephone network, where a dedicated end-to-end transmission path (*i.e.* a circuit) must be opened for each transmission. Packet-switched systems enable network resources (*i.e.* the

[1] On the technical aspects of the internet, see Werbach, "Digital Tornado: The Internet and Telecommunications Policy" (1997) 3 *OPP Working Paper Series*, available at: *http://www.fcc.gov/Bureaus/Wireless/OPP/working_papers/oppwp29pdf.html*; Hance, *Business and Law on the Internet* (1997), 41; and Wilde, *Wilde's WWW: Technical Foundations of the Worldwide Web* (1999).

[2] See Werbach, para.3–001, n.1, 13–16; and Hance, para.3–001, n.1, 40.

available bandwidth) to be used more efficiently, as they enable a greater volume of data to be carried on the same transmission facilities.[3]

3–002 Key players—Viewed simplistically, the technical operation of the internet involves four different players: end-users, content providers, internet access service providers (ISPs) and backbone or "top-level network" providers. End-users access the internet through either dial-up or dedicated (*i.e.* "always on") connections to access information or purchase services supplied by content and service providers.[4] ISPs connect end-users to internet backbone networks, while backbone providers route traffic between ISPs and interconnect with other backbone providers. Interconnection between backbone or top-level internet connectivity providers has been traditionally effected through so-called "peering" agreements, *i.e.* barter arrangements between backbone providers in which they exchange traffic between themselves without payment provided that the ratio of exchanged traffic is within certain limits. Secondary internet connectivity providers (or second-tier providers) may be able to deliver some of their own peering-based connectivity, but usually have to supplement it through transit bought from the top-level networks.[5] The reality is more complex, as certain backbone operators also act as ISPs, and some large corporate end-users connect directly to backbone providers.

3–003 The internet is a prime driver of convergence—The internet's distinctive feature is its technical architecture. This has been a primary factor behind the process of convergence of telecommunications and broadcasting networks and IT systems. The use of an open protocol ensures network interconnectivity and, with any necessary technical adjustments, the provision of any type of information (*i.e.* voice, images and data) on any type of network (*e.g.* cable, public telephone networks and wireless networks). Internet-based services are, therefore, distinct from the underlying infrastructure on which they are transmitted. Accordingly, the internet competes with traditional transmission networks (such as broadcasting, telecommunications and other data communications services) by providing an alternative means of distributing services and content. For example, the internet can now be used to distribute television or radio programmes, voice telephony and software, in competition with the traditional channels of distribution. In this way, the internet has greatly contributed to bringing together the telecommunications, broadcasting and

[3] This may raise a quality problem for services such as voice telephony or video that require a constant level of transmission, as some packets can be lost or delayed. However, improvements in IP networks technology now permit speech and video to be successfully transmitted.

[4] Despite significant growth in the availability and use of broadband access, narrowband dial-up access to the internet remains an important end-user product. In 2007, 30% of the households in the EU27 that used the internet used narrowband access, according to a Special Eurobarometer E-Communications survey of April 2007: see Commission Recommendation 2007/879 of December 17, 2007 on relevant product and service markets within the electronic communications sector susceptible to *ex ante* regulation in accordance with Directive 2002/21 of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (2nd ed.), O.J. 2007 L344/65, in particular its Explanatory Memorandum, SEC(2007) 1483/2, 36, available at *http://ec.europa.eu/information_society/policy/ecomm/library/recomm_guidelines/index_en.htm*.

[5] The decision of the European Commission in Case M.1069, *WorldCom/MCI*, Commission Decision of July 8, 1998 (discussed in para.7–237 *et seq.*), contains a detailed description of the working of interconnection arrangements between ISPs and backbone providers. The European Commission's subsequent decision in Case M.1741, *MCI WorldCom/Sprint*, Commission Decision of June 28, 2000 (discussed in para.7–258 *et seq.*) noted that while there had been a number of technical developments since its earlier decisions, these developments had not had any significant impact on the structure of the market or on interconnection agreements between backbone providers of universal connectivity and other ISPs.

IT sectors, which were historically separate because they used different delivery vehicles.[6] In this context, the convergence brought about by the internet has raised the question of whether the regulatory regimes applicable to traditional media (such as telecommunications and broadcasters) should be extended to internet-based services.

3–004 Web 2.0—While the primary internet services initially included electronic mail (or email), the World Wide Web ("www"), Telnet, File Transfer Protocol ("FTP"), Gopher and newsgroups,[7] the current "Web 2.0" phenomenon is rapidly changing the range and scope of services offered online. "Web 2.0" can be described as a second generation of internet-based services that emphasise online collaboration and sharing among users (*e.g.* online video portals and other sharing sites, online social networks, wikis and other forms of collective intelligence, blogs, podcasts, etc.). It has a fundamental impact in the architecture of communications and media in general and by extension in the way citizens engage and participate in their societies. Whereas the world wide web was seen as the principal factor in the exponential growth of internet use for the purpose of electronic commerce ("e-commerce"), the concept of Web 2.0 is seen as leading to a paradigm shift in communications and social interaction. At its heart is the idea that users are not just browsing and consuming content in the traditional media fashion, but they participate, contribute, create, reuse, repurpose, rank, link, and share the content with other users, generally at a global scale.[8]

3–005 Legal issues raised by the internet—The emergence of the internet as a major vehicle for cross-border communications, particularly of converged services, raises a number of complex legal issues. Indeed, the novelty and uniqueness of the phenomenon continue to challenge the application of existing laws in many areas. It has even been claimed that the evolving internet faced a legal vacuum and that there was a need to urgently develop a new regulatory framework specifically for it. Although, as is discussed below in greater detail, specific regulatory intervention is clearly needed in certain respects, many of the legal questions raised by the use of the internet may be solved, to a large extent, by the application of existing laws. A review of all legal questions raised by the use of the internet, many of which (*e.g.* liability on the internet, conflict of laws, rules of evidence, contractual issues and the application of criminal law) continue to fall largely within the ambit of national laws, is beyond the scope of this work.[9] This chapter focuses on a number of specific regulatory issues raised by the internet and reviews how these issues have been addressed by legislation at the EU level.

[6] Werbach, para.3–001, n.1, 1–8. For an analysis of the impact of the internet on the telecommunications sector, see Gilhooly, "Towards the Global Internet Infrastructure" (1999) 3 *International Journal of Communications and Policy* 1.

[7] See Hance, para.3–001, n.1, 42–46.

[8] See Ariño, "Content Regulation and New Media: A Case Study of Online Video Portals" (2007) 66 *Communications and Strategies* 115–135.

[9] See, for example, the following commentaries, which have extensively reviewed these matters: Hance, para.3–001, n.1; Gringras, *The Laws of the Internet* (3rd ed., 2008); Lloyd, *Information Technology Law* (5th ed., 2008); Johnston, Handa and Morgan, *Cyberlaw: What You Need to Know about Doing Business Online* (1997); and Chissick and Kelman, *Electronic Commerce: Law and Practice* (3rd ed., 2002). For a review of the treatment of these issues in the national laws of various European, Asian and North American countries, see Dumortier (ed.), *International Encyclopaedia for Cyber Law*, available at *http://www.ielaws.com/cyber.htm*; and Smith, *Internet Law and Regulation* (2002).

B. Internet governance: naming and addressing

3–006 The domain name system—The issue of internet governance and regulation remains a subject of controversy and intense debate among the different actors within the internet community.[10] Some take the position that the internet should not be regulated at any level, whether national or international, whilst others consider that a minimum degree of regulation is necessary to address certain issues that cannot be left exclusively to competitive forces and self-regulation.[11] Every computer connected to the internet has a unique IP address, which is a number that identifies it to other computers.

3–007 ***Domain name hierarchy***—The domain name system (DNS) maps user-friendly names onto these numbers, which are difficult to remember. The domain name space is constructed as a hierarchy. It is divided into so called top-level domains (TLDs). Most TLDs carry a country code (ccTLDs) and refer to a country or distinct territory (*e.g.* ".be" for Belgium, ".uk" for the United Kingdom, ".de" for Germany, etc.), while a small set of top-level domains (gTLDs) do not carry any national identifier, but denote the intended function of the domain space (*e.g.* ".com" for commercial organisations, ".org" for non-profit organisations and ".int" for international organisations). Generally, ccTLD extensions have only two letters, while gTLD extensions have three or more. It should be noted that important changes have been adopted and the anticipation is that the number of gTLDs will grow significantly from 2010 or 2011 onwards. Each TLD can, in turn, be divided further into second level domains (SLDs), such as ".co.uk".

3–008 ***Registration of domain names***—To register a domain name, a registrant (*i.e.* a person or company desiring to register a domain name or being the holder of such a domain name) must first provide a registrar (*i.e.* a service provider that acts as an intermediary between registrants and registries for the registration and management of domain names) with the contact and technical information that makes up the registration and enter into a registration contract with the registrar. The registrar keeps a record of the contact information and submits the technical information to a central directory, known as a registry. A registry is an entity that receives domain name service information from domain name registrars, inserts that information into a centralised database and propagates the information in internet zone files on the internet so that domain names can be found by users around the world.

3–009 Background to the domain management structure—Historically, the internet developed as a result of the efforts of the US government to set up an advanced data communications infrastructure for the purposes of national security and research. As a result of this legacy, management of the internet has traditionally been based in the United States, with major components of the domain name system performed by or subject to agreements with US government agencies, including the Defence Advanced Research Project Agency (DARPA) and the National Science Foundation (NSF). Until 1998, the registration and allocation of gTLDs was managed by the Internet Assigned Numbers Authority (IANA), and Network Solutions, Inc. (NSI), under contract

[10] See, for an earlier discussion, Issgon, Grewlich and Di Pietrantonio, "Competing Telecommunications and Cyber Regulation: Is there a Need for Transatlantic Regulatory Framework?" (1999) 3 *International Journal of Communications Law and Policy* 1.

[11] See Kelleher, "Generic Domain Names on the Internet" (1998) 20(2) E.I.P.R. 62; and Mathiason and Kuhlman, "International Public Regulation of the Internet: Who Will Give You Your Domain Name?", March 1998 in *International Studies Associations Panel on Cyberhype or the Deterritorialization of Politics?*, available at: *http://www.intlmgt.com/domain.html.*

to the US government. Under this arrangement, IANA/NSI acted as the sole registry for and registrar of .com, .net and .org domains worldwide.

3–010 Amendments to the domain management structure—As the international use of the internet grew and became more commercialised, a general consensus emerged in the internet community that the IANA/NSI registration and allocation system was inadequate to ensure the smooth operation of the internet. In particular, there was widespread dissatisfaction about the absence of competition in domain name registration. In addition, existing mechanisms for resolving conflicts between trademark owners and domain name holders were considered to be both cumbersome and expensive. Finally, as the internet became more and more international, there was dissatisfaction outside the United States, especially in Europe, that internet domains and new top-level domains were allocated by US-based entities that were neither representative of, nor accountable to, the general internet community. As a result, several initiatives were launched in order to identify the most appropriate structure for regulating the DNS.[12] These initiatives resulted in the US government initiating a public consultation in the course of 1997. This resulted in the publication of a Green Paper on Internet Governance in January 1998.[13] In essence, the US Green Paper proposed to remove, after a transitional period, the US government from any role in internet governance and to replace IANA with a US-based private, non-profit corporation. The EU was very critical of the proposals contained in the US Green Paper, because they did not ensure an appropriate representation of non-US interests at the board level of the new entity to be entrusted with the management of domain names. The US government amended its initial proposals to accommodate these objections. In June 1998, it issued a policy statement in the form of a White Paper, setting out the different steps for the reform of the organisation and management of the DNS.[14]

3–011 Creation of new managing entity for the domain name system—The Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation, was incorporated in the United States on October 1, 1998. It succeeded IANA in administering the DNS. Representation at the board level of ICANN is organised so as to ensure balanced and representative participation from the various actors of the internet community, on both a functional and geographic level.

3–012 Competitive registrars and registries—ICANN has managed the transition of the DNS from a government-sanctioned monopoly to a competitive market in which the DNS is operated by private businesses. The key element of this liberalisation process was the accreditation by ICANN of a potentially unlimited number of competitive, market-driven registries and registrars for the gTLDs.

[12] A Memorandum of Understanding was signed in 1997 within the framework of the International Ad-Hoc Committee (IAHC), a committee composed of representatives of different organisations including IANA, the International Telecommunications Union (ITU) and the World Intellectual Property Organisation (WIPO). The Memorandum of Understanding recommended a new structure for the management and administration of the DNS, based on a self-regulating market: see Kelleher, para.3–006, n.11, and Mathiason and Kulhman, para.3–006, n.11.

[13] US Green Paper on Internet Governance, "A Proposal to Improve Technical Management of Internet Names and Addresses", January 30, 1998.

[14] US Department of Commerce, "Management of Internet Names and Addresses", Statement of Policy, June 5, 1998, Docket Number: 980212036-8146-02. The changes in policy brought about by the US White Paper were largely welcomed by the European Commission: Communication from the Commission, "Management of Internet Names and Addresses: Analysis and Assessment from the European Commission of the U.S. Department of Commerce White Paper", COM(1998) 476 final.

3–013 ***Shared Registration System protocol***—In order to implement this system and allow for competing registrars, NSI (now called VeriSign) developed the Shared Registration System (SRS) protocol and associated hardware and software to permit multiple registrars to provide registration services for the existing gTLDs. VeriSign licenses this protocol and software to registrars by way of a standard licensing agreement. The first phase of this process, the "test-bed" phase, ran from March to November 1999.

3–014 ***Accredited registrars***—In April 1999, VeriSign accredited five registrars (America Online, CORE, France Télécom, Melbourne IT and register.com) to take registrations in the .com, .net and .org gTLDs. These registrars began live operations in June 1999.[15] Shortly thereafter, ICANN began accepting applications from a potentially unlimited number of registrars. Currently there are nearly 1000 accredited registrars.[16] ICANN also managed to change VeriSign's dominant position as registry for the most important commercial gTLDs .com, .org and .net. In 2001 VeriSign was awarded a new contract with ICANN to operate the .com TLD for a period of six years. In 2006 a new contract was negotiated between the two parties allowing VeriSign to remain as the registry for the .com TLD until November 30, 2012. One year earlier VeriSign also managed to remain as the registry for the .net TLD (until June 30, 2011). However, VeriSign was not reconfirmed as the registry for the .org TLD. In 2002 ICANN and Public Interest Registry (PIR) entered into a registry agreement that attributed the management of .org to PIR for a period of six years. In December 2006, ICANN and PIR renewed the registry contract for .org confirming PIR as the registry till June 30, 2013.

3–015 **Creation of new gTLDs**—A number of new gTDLS have been progressively introduced since 2000.

3–016 ***2000: seven new gTLDs***—In November 2000, ICANN adopted seven new gTLDs: .aero (a restricted gTLD for the air transport industry), .biz (an open gTLD for businesses), .coop (a restricted gTLD for use by cooperatives), .info (an open gTLD that will compete with .com), .museum (a restricted gTLD for use by museums), .name (a gTLD restricted to individuals) and .pro (a restricted gTLD for the legal, medical and accounting professions).

3–017 ***2003: proposals for new gTLDs***—In December 2003, ICANN launched a request for proposals for new gTLDs. It received ten applications and ultimately the following new gTLDs were approved (in 2005 and 2006) by the ICANN Board: .asia (a community based TLD for Asian businesses and individuals), .cat (a community based TLD for the Catalan region in Spain), .mobi (a gTLD for the mobile communications industry), .tel (a gTLD that aims to offer eNUM like services), .travel (a restricted gTLD for the travel industry), and .jobs (a restricted gTLD for human resources management). All of these gTLDs are currently operational and are currently accepting registrations. In June 2008, ICANN adopted the recommendations of its Generic Names Supporting Organisation (GNSO) on a new gTLD programme.

3–018 ***2008: draft ICANN Applicant Guidebook***—In October 2008, ICANN released a draft Applicant Guidebook for public comment.[17] An analysis of over 300 comments to the Guidebook resulted in substantial changes, reflected in a second draft of the Guidebook which was published in February 2009 and which initiated a new public comment period. In October 2009, a third version of the Applicant Guidebook was issued, but numerous problems still seem to be

[15] Information on the accreditation guidelines and process is available at: *http://www.icann.org/registrars/accreditation.htm*.

[16] A list of accredited registrars is available at: *http://www.icann.org/registrars/accredited-list.html*.

[17] For a full overview of the new gTLD programme and the draft Applicant Guidebook, see *http://www.icann.org/en/topics/new-gtlds/comments-en.htm*.

unresolved. Currently there is no clear timeline, but the first series of new gTLDs will probably not be added to the root zone before mid-2011. Unlike the two previous application rounds for new gTLDs, where only a limited number of proposals were adopted, ICANN aims to set up a general application model that will serve as a framework for the evaluation of a theoretically unlimited number of new gTLD proposals. It is expected that the outcome of this process will lead to the addition of a large number of new gTLDs (estimates vary from a few dozen to several hundred) to the root zone in the next couple of years.

3–019 **Creation of the .eu ccTLD**—One of the key elements of the eEurope 2002 Action Plan launched at the Lisbon Summit of 2000 was the establishment of the .eu TLD to supplement existing ccTLDs and gTLDs. After a lengthy consultation process with the Member States, on April 22, 2002, the European Parliament and the Council adopted the Regulation on the implementation of the .eu top-level domain.[18] This Regulation provides for the designation of a registry that will manage the .eu TLD, the obligations of the registry and the general public policy framework for the implementation and functions of the .eu TLD, for example, on extra-judicial dispute settlement and the treatment of intellectual property rights.[19] On May 22, 2003, the Commission designated EURID—the European Registry for Internet Domains—as the registry for the .eu ccTLD.[20] The regulatory framework for the .eu TLD was further completed in April 2004 with the adoption of the Regulation on Public Policy Rules.[21] This Regulation sets out the general principles for the domain name registration policy, the accreditation of registrars, some specific rules for geographical and geopolitical names, the phased registration ("sunrise period") and validation of applications introduced during the phased registration and the alternative dispute resolution procedures. The .eu ccTLD was added to the root zone in March 2005. The sunrise period started in December 2005 and general registrations began in April 2006.

C. Licensing and other market entry restrictions for internet services

1. Licensing of internet-based services

3–020 **Internet service providers under the Electronic Communications Regulatory Framework**—Any undertaking wishing to provide services on the internet must consider whether its proposed

[18] Regulation 733/2002 of the European Parliament and of the Council of April 22, 2002 on the implementation of the .eu Top Level Domain, O.J. 2002 L113/1. The .eu TLD is now available in all 23 official EU languages: see Commission Press Release, *".eu" internet domain now available in all EU languages*, IP/09/1903 (December 10, 2009). In addition to the use of the standard Latin characters "a to z", "0 to 9" and "-", domain names can now also be registered using characters from the alphabets of different national languages, including the non-Latin Greek and Cyrillic alphabets, including characters such as "à", "ą", "ä", "ñ", "ç", "ψ" or "я". This is possible because the ".eu" TLD is now an Internationalised Domain Name. As at September 20, 2009, EURid, which operates the ".eu" domain, had registered 2,991,205 domain names using the ".eu" TLD, with Germany, the Netherlands and the United Kingdom having the largest number of ".eu" domains.

[19] *ibid.*, Arts.3–5.

[20] Commission Decision 2003/375 of May 21, 2003 on the designation of the .eu Top Level Domain Registry, O.J. 2003 L128/29.

[21] Commission Regulation 874/2004 of April 28, 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration, O.J. 2004 L162/40.

activities are subject to any licensing or market entry conditions in the country in which it will provide its services. The answer to this question depends on the nature of the activity undertaken. In the EU, the regulatory regime applicable to the internet varies according to the nature of the undertaking's activities. The EU regulatory framework explicitly divides internet-related services into two categories, namely electronic communications services (i.e. transport of signals) and information society services (more focusing on content-related issues).

3–021 ***Electronic communications services***—The first category, electronic communications services, is defined in the Framework Directive as services normally provided for remuneration which consist wholly or mainly in the conveyance of signals on electronic communications networks. This excludes services providing, or exercising editorial control over, content using electronic communications networks and services, and information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks (*i.e.* most information society services).[22] Electronic communications services include internet access services and the conveyance of email.[23] The same undertaking can provide both electronic communication services (such as internet access) and information society services (such as web-based content).[24] The provision of electronic communications services is normally subject only to a general authorisation, in accordance with the provisions of the Authorisation Directive.[25] Member States may require ISPs to obtain individual rights of use in order to use radio frequencies (*e.g.* to provide internet access over wireless networks) or numbers (*e.g.* to provide dial-up or broadband internet access over their own networks), where this is necessary to allow efficient access to, and use of, radio frequencies and/or numbers.[26] However, these provisions are unlikely to be relevant to most ISPs, as they generally do not use their own networks to provide internet access services and thus do not require their own frequencies or numbers.[27]

3–022 ***Information society services***—Information society services (or e-commerce services) are the second category. Information society services are defined in the E-commerce and Transparency Directives as any service normally provided for remuneration, at a distance (*i.e.* without the parties being simultaneously present), by electronic means (*i.e.* by means of electronic equipment for the

[22] Directive 2002/21 of March 7, 2002 on a common regulatory framework for electronic communications networks and services, O.J. 2002 L108/33 ("Framework Directive"), amended by Directive 2009/140 of November 25, 2009 amending Directives 2002/21, 2002/19 and 2002/20 ("Better Regulation Directive"), O.J. 2009 L337/37, Art.2(c).

[23] Framework Directive, para.3–021, n.22, recital 10.

[24] *ibid.*

[25] Directive 2002/20 of March 7, 2002 on the authorisation of electronic communications networks and services, O.J. 2002 L108/21 ("Authorisation Directive"), amended by the Better Regulation Directive, para.3–021, n.22, Art.3.

[26] Authorisation Directive, para.3–021, n.25, Art.5.

[27] The former European Radiocommunications Office (ERO), now merged with the European Telecommunications Office (ETO) into the European Communications Office (ECO), has offered a "one-stop shopping" procedure for satellite authorisations for some years. ISPs providing their services over satellite networks could avail themselves of this procedure, enabling them to obtain a general authorisation in multiple Member States by virtue of submitting a single application to ERO. Although the ERO invested considerable efforts in preparing a database and creating a coherent approach towards applications for satellite earth station authorisations, it had to end the procedure in 2004, due to difficulties of coordinating forms and formats for applications: see Hogan & Hartson and Analysys, *Preparing the next steps in regulation of electronic communications, Study for the European Commission* (July 2006), 209, available at: *http://ec.europa.eu/information_society/policy/ecomm/doc/info_centre/studies_ext_consult/next_steps/regul_of_ecomm_july2006_final.pdf*.

processing, including digital compression, and storage of data and entirely transmitted, conveyed and received by wire, radio, optical or other electro-magnetic means) and at the individual request of the recipient of services.[28] Information society services include the provision of web-based content and e-commerce services. Most information society services are not within the scope of the Electronic Communications Regulatory Framework, as they do not involve wholly or mainly the conveyance of signals on electronic communications networks. The Electronic Communications Regulatory Framework in principle does not apply to the provision of internet content[29] or to other information society services, which are within the scope of the E-Commerce Directive.[30] However, ISPs and other undertakings that provide both content and other information society services and also electronic communications services are subject to both the Electronic Communications Regulatory Framework and the E-Commerce Directive.[31]

3–023 Internet backbone providers—Internet backbone providers operate high capacity broadband networks. These are electronic communications networks under the Electronic Communications Regulatory Framework.[32] Therefore, the provision of internet backbone services, or universal or top-level connectivity, is subject to the general authorisation regime laid down in the Authorisation Directive[33] and, if radio frequencies or numbers are used, potentially also to the individual rights of use.[34] If internet backbone providers are public communications networks within the meaning of the Framework Directive,[35] they would additionally have the rights and the obligations on access and interconnection contained in the Access Directive.[36] However, generally, it is unlikely that internet backbone providers would be subject to the *ex ante* regulatory regime for operators that have been designated as possessing SMP under the terms of the Framework Directive.[37] This is because internet backbone providers' services should not be considered to be

[28] Directive 98/34 of June 22, 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, O.J. 1998 L204/37, as amended by Directive 98/48 of July 20, 1998, O.J. 1998 L217/18 ("Transparency Directive"), Art.1(2). An illustrative list of services that are not considered to be information society services can be found in Annex V of the Directive, and includes voice telephony, telephone consultations with a lawyer or doctor, and radio and television broadcasting services.

[29] Framework Directive, para.3–021, n.22, recital 5; Directive 2002/19 of March 7, 2002 on access to, and interconnection of, electronic communications networks and associated facilities, O.J. 2002 L108/7 ("Access Directive"), recital 2. The Access Directive is amended by the Better Regulation Directive 2009, para.3–021, n.22.

[30] Directive 2000/31 of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, O.J. 2000 L178/1 ("E-Commerce Directive"). For a discussion of the E-Commerce Directive, see para.3–114, *et seq.*, below.

[31] Framework Directive, para.3–021, n.22, recital 10.

[32] *ibid.*, Art.2(a).

[33] Authorisation Directive, para.3–021, n.25, Art.3.

[34] *ibid.*, Art.5.

[35] Framework Directive, para.3–021, n.22, Art.2(d).

[36] Access Directive, para.3–022, n.29, Art.4. The Access Directive does not specifically define the terms "public" or "publicly available". However, recital 1 of the 2002 Access Directive states that operators of non-public networks do not have obligations under the Access Directive except if they benefit from access to public electronic communications networks, in which case they may be subject to conditions laid down by Member States.

[37] Framework Directive, para.3–021, n.22, Art.16. Annex I of the 2002 Framework Directive did not include the provision of internet backbone services, or "wholesale internet connectivity", in the list of markets on which the Commission had to base its first Recommendation on Relevant Markets. In the Explanatory Memorandum to the 2003 Recommendation on Relevant Markets, the Commission offers its rationale for not subjecting markets for wholesale internet connectivity to *ex ante* regulation by NRAs: Explanatory

"publicly available", as their customers are ISPs and large businesses, rather than the public at large. Similarly, on this basis, internet backbone providers would not be subject to universal service obligations, because they do not operate public telephone networks or provide publicly available telephone services.[38]

3–024 Content providers—The internet can be used to provide a great variety of services, including content services. The licensing regime applicable to services or information provided over the internet thus depends on the nature of the service or content in question. Information society services (other than those that consist wholly or primarily in the conveyance of signals on electronic communication networks) such as web-based content, e-commerce and web-hosting, are covered by the E-Commerce Directive[39] and possibly also the Audiovisual Media Services Directive.[40]

3–025 ***Country of origin principle***—Internet services are subject to regulation only by the Member State in which the service provider is established under the "country of origin" principle;[41] providers of such services may not be subject to any prior authorisation regime specifically aimed at information society services as such.[42] This does not mean that providers of services over the internet are exempted from generally applicable rules simply by virtue of using the internet. For example, a lawyer providing legal advice over the internet is still subject to generally applicable national rules requiring him to be a member of the relevant Bar, but Member States may not impose any additional obligations over and above those applicable to lawyers in general for him to provide his services by means of the internet. Similarly, services that are generally prohibited or regulated in a given Member State, *e.g.* gambling, would also be prohibited or regulated online.[43] Certain services are excluded from the scope of the E-Commerce Directive.[44] Other services which are not provided by electronic means do not come within the scope of the E-Commerce Directive and remain subject to existing regulatory regimes under national and/or EU law.

Memorandum to Commission Recommendation of February 11, 2003 on the relevant product and service markets within the electronic communications sector susceptible to *ex ante* regulation in accordance with Directive 2002/21 of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services, O.J. 2003 L114/45, 27, available at *http://ec.europa.eu/information_society/policy/ecomm/library/recomm_guidelines/index_en.htm*. The Commission adopts the same reasoning in its 2007 Recommendation on Relevant Markets, Explanatory Memorandum, 37, para.3–002, n.4; hence, it again concludes that entry barriers to the market for wholesale internet connectivity are low and that there is no *a priori* presumption that *ex ante* market analysis is required. Although NRAs could possibly identify additional markets for the purposes of identifying operators with SMP, no NRA has defined such market for internet backbone services.

[38] Directive 2002/22 of March 7, 2002 on universal service and users' rights relating to electronic communications networks and services, O.J. 2002 L108/51 ("Universal Service Directive"), amended by Directive 2009/136 of November 25, 2009 amending Directive 2002/22, Directive 2002/58 and Regulation (EC) 2006/2004 on consumer protection cooperation (Citizens' Rights Directive), O.J. 2009 L337/11, Art.2(b) and (c).

[39] E-Commerce Directive, para.3–022, n.30. For a discussion of the E-Commerce Directive, see para.3–114, *et seq.*, below.

[40] See para.3–028 *et seq.*, below.

[41] E-Commerce Directive, para.3–022, n.30, Art.3(1) and (2).

[42] *ibid.*, Art.4(1).

[43] *ibid.*, Art.1(5)(d).

[44] *ibid.*, Art.1(5)(d). The E-Commerce Directive does not apply to: (i) the activities of notaries and other professions to the extent that they involve a direct and specific connection with the exercise of public authority; (ii) the representation of a client and reference of his interests before the courts; and (iii) gambling activities (including lotteries and betting transactions).

3–026 ***Derogations from country of origin principle***—Member States may derogate from the "country of origin" principle and may continue to apply national laws to providers of information society services established in other Member States, in the following areas: copyright, neighbouring rights and other intellectual and industrial property rights; the issuing of electronic money by some institutions; the freedom of parties to choose the applicable law of their contract; contractual obligations concerning consumer contracts; rules on the formal validity of contracts creating or transferring interests in land; unsolicited commercial communications by email; measures necessary for public policy reasons (in particular the prevention, investigation, detection and prosecution of criminal offences; the protection of minors; the prevention of incitement on the grounds of sex, race, religion and nationality; and the protection of human dignity); measures for the protection of human health; measures for the protection of public security; and measures for the protection of consumers, including investors.[45]

3–027 Web-casting—In the context of convergence, it is interesting to review the status of web-casting, which straddles the line between internet and broadcasting services, just like IP voice telephony straddles the line between internet and telecommunications services, as will be discussed below. Web-casting services, which consist of the provision of real-time radio or video services over the internet, are readily available. Although real-time video broadcasting is presently still limited to users with high-speed connections, it is expected that internet technologies, such as IP multi-casting,[46] will permit the widespread use of the internet as a major means of transmitting audio and video. Most traditional broadcasters already offer a wide range of online services, which are complementary to their linear services (*e.g.* news services, catch up services, educational services).[47] The fast-growing popularity of online video portals, such as YouTube, and other services which are characteristic of the Web 2.0 phenomenon (such as social networking sites and wikis)[48] demonstrate the growing convergence between the internet and traditional broadcasting services. This raises the question of whether the strict licensing conditions and other regulatory restrictions applicable to the broadcasting sector (*e.g.* regarding licensing, programming, European content quotas and levels of advertising) apply to analogous internet-based services, or whether web-casting should be treated as an information society service for which prior authorisation is excluded by the E-Commerce Directive.

3–028 ***Scope of AVMS Directive***—In 2007, the European Parliament and Council have broadened the scope of the former Television Without Frontiers Directive[49] considerably, to

[45] *ibid.*, Arts.3(3) and 3(4).

[46] IP multicasting is a method of forwarding IP data sets ("datagrams") to a group of multiple receivers and is used for streaming media and internet television applications. IP multicasting has been officially supported since IPv4 was first defined, but has not seen widespread use, due largely to lack of support for multicasting in many *hardware* devices. Interest in multicasting has increased in recent years, and support for multicasting was made a standard part of the next generation IPv6 protocol.

[47] The most advanced broadcaster in this respect is probably the British public broadcaster, the BBC, which offers its own "BBC iPlayer", service allowing United Kingdom residents to view the radio and television programmes broadcast in the previous seven days (and also offers download and limited storage possibilities) by connecting to its website (currently operable with a computer using Windows, Macs, or Linux; a Nintendo Wii; and an iPhone): see *http://www.bbc.co.uk* and *http://www.bbc.co.uk/iplayer*.

[48] See para.3–001, above. For an interesting analysis of these new portals from the perspective of content regulation, see: Ariño, "Content Regulation and New Media: A Case Study of Online Video Portals" (2007) 66 *Communications and Strategies* 115–135.

[49] Directive 89/552 of October 3, 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities, O.J. 1989 L298/23 ("Television Without Frontiers (TWF) Directive").

include not only linear but also non-linear (on-demand) services. The new Audiovisual Media Services Directive applies to all audiovisual media services, which are services in the sense of Articles 56 and 57 of the Treaty on the Functioning of the European Union [ex 49 and 50 EC Treaty] which come under the editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes in order to inform, entertain or educate, to the general public by electronic communications networks.[50] However, taking account of the various constituent elements of audiovisual media services, it has become clear that not all media services that are currently offered via the internet will fall within the scope of the AVMS Directive.[51] It is, for example, unlikely that online video portals, to which users can upload and share videos ("user-generated content"), will qualify as an audiovisual media service: even if the provider is carrying out an economic activity and, hence, is to be considered providing a service in the sense of Article 56 and 57 , it is usually not exercising effective control both over the selection of the programmes and over their organisation and so does not have "editorial responsibility" for the service.[52]

3–029 ***Graduated regulation for online services***—Media services offered online that fulfil all the criteria of an audiovisual media service will, depending on the format used, either be subject to the lighter rules applicable to on-demand services, or to the stricter rules applicable to linear services, given the system of graduated regulation in the AVMS Directive.[53]

3–030 ***Non-linear content***—Web-cast content that is provided to users on demand (*i.e.* where transmission is initiated upon the individual user's request, such as with video-on-demand), would qualify as non-linear services, and hence be subject to the basic tier of regulation in the AVMS Directive, as well as being subject to the E-Commerce Directive.[54]

3–031 ***Linear content***—Web-cast content that is transmitted simultaneously to multiple users who have not made an individual request (*e.g.* where the film, song, etc., is broadcast automatically at regular intervals, as in pay-per-view systems, or where a web-caster continually broadcasts a selection of content in the same way as a terrestrial radio station, involving the broadcasting of a pre-determined program schedule to the public), would qualify as a linear service and would thus also be subject to the additional tier of stricter provisions contained in the AVMS Directive.

3–032 ***Technologically-neutral approach to regulation***—The European legislature has opted for a technologically neutral approach to broadcasting regulation, such that internet broadcasting can also be subject to regulation. It did so to create a level playing field between traditional and new media providers and to ensure an appropriate level of protection for certain essential public interests, such as cultural diversity and protection of minors. However, the extension of the scope of application of the regulatory regime laid down in the TWF Directive met fierce opposition during the legislative process for the AVMS Directive from new media providers in the online and

[50] Directive 2010/13 of December 11, 2007 amending Directive 89/552, O.J. 2007 L332/27 ("AVMS Directive"), Art.1(a).

[51] See para.2–029 *et seq.*

[52] AVMS Directive, para.3–028, n.50, Art.1(c): see Chapter II, para.2–031, above. For a discussion of the legal status of video portals and audiovisual search tools, see Valcke, "In Search of the Audiovisual Search Tools in the EU Regulatory Frameworks", in Nikoltchev (ed.), *IRIS Special: Searching for Audiovisual Content, Strasbourg, European Audiovisual Observatory* (European Audiovisual Observatory, 2008).

[53] See para.2–057 *et seq.*, above.

[54] On-demand media services are also information society services (as they were before the adoption of the AVMS Directive) and, consequently, are still subject to the E-Commerce Directive, para.3–022, n.30, recital 18. Art.4(8) of the AVMS Directive deals with the relationship between both directives, stating that the AVMS Directive will prevail in the event of a conflict, unless otherwise provided for. Therefore, the AVMS Directive has the character of a *lex specialis* vis-à-vis the E-Commerce Directive, which is a *lex generalis*.

mobile sectors, as well as certain Member States, such as the United Kingdom.[55] Criticism was also voiced by some media scholars, expressing concerns about a possible negative impact on freedom of speech that would result from the AVMS Directive's broadened—and in their view too vague—scope of application.[56] The AVMS Directive, however, does take into account the different nature and impact of online media services (which will often be on-demand services), by subjecting them to a lighter regime[57] and permitting the use of co- and self-regulatory measures.[58] Therefore, it seems unlikely that the AVMS Directive will result in disproportionate regulation being imposed on internet broadcasters.[59] Moreover, it may even lead to more legal certainty for online media providers, who can now clearly benefit from the country of origin principle in relation to the content requirements covered by the AVMS Directive, as if they comply with the rules of the Member State in which they are established, they can freely offer their services throughout the EU.[60]

3–033 **Voice over Internet Protocol**—With respect to IP voice telephony (or "Voice over IP"), as technology gradually improved its quality and made it equivalent functionally to traditional voice telephony services, the question arose as to whether IP voice telephony should be subject to the same licensing and regulatory requirements applicable to traditional voice telephony.[61]

[55] See Valcke and Lievens, "Rethinking European Broadcasting Regulation: The Audiovisual Media Services Directive Unraveled at the Dawn of the Digital Public Sphere", in Pauwels, Kalimo, Donders and van Rompuy (eds.), *Rethinking European Media and Communications Policies* (2009).

[56] See, for example, the Budapest Declaration (2006): "the extension of the scope of some rather burdensome part of the Television Directive to the Internet—as the draft new directive of the European Commission suggests in far too vague terms that would leave content providers and users uncertain about whether or not their various activities are regulated by this new directive—would be an unjustifiable restriction on freedom of speech and freedom of information", available at *http://www.edri.org/docs/BudapestDeclaration.pdf*. These scholars feared that governments might (mis)use the new AVMS Directive as an excuse to impose strict regulations on any kind of information exchanged via the internet, which in their view should remain an entirely "free medium". See also van Eijk, "The modernisation of the European Television without Frontiers Directive: unnecessary regulation and the introduction of internet governance", paper presented at the 19th European Regional Conference of the International Telecommunications Society, Istanbul, September 2–5, 2007, available at: *http://www.ivir.nl/publications/vaneijk/Paper_twf_avms_its_2007.pdf*.

[57] Consisting of obligations which are often already imposed by other legislations: see Valcke, Stevens, Werkers and Lievens, "Audiovisual Media Services in the EU: Next Generation Approach or Old Wine in New Barrels?" (2008) 71 *Communications & Strategies* 103–118.

[58] See para.2–122, above.

[59] It has been argued that the rationale for strict broadcasting regulation (*i.e.* spectrum scarcity and general public access to broadcasts) does not necessarily apply to equivalent internet-based services. For instance, the technical architecture of the internet permits the implementation of filtering techniques that allow users, such as parents, to block access to certain sites, thereby achieving the objective of traditional rules on protection of minors that regulate the broadcasting sector: see Werbach, para.3–001, n.1, 44. To justify the imposition of lighter rules, the AVMS Directive explicitly refers, in recital 42, to the larger degree of choice and control the user can exercise in the case of on-demand services, and the lower impact they have on society.

[60] Admittedly, due to the decentralised nature of the internet, media regulators in the European Union might still have limited abilities to enforce regulatory restrictions upon content providers that supply services over the internet from third countries.

[61] Voice over Internet Protocol ("VoIP") is the delivery of voice and other services over networks based wholly or partly on Internet Protocol (IP). As far as the IP-based part of the network is concerned, the VoIP packets may be transmitted on public internet segments, managed IP networks, or both. As a result, the quality of service (QoS) may vary. The European Regulators Group divided VoIP services into four categories, depending on whether or not there is access to or from the public switched telephone network ("PSTN") and whether or not E.164 numbers are used (*i.e.* numbers from the international telephone

3–034 ***Commission Staff Working Document on VoIP***—While the Commission initially, in 1998,[62] considered that telephony should not be subjected to the regulatory regime applicable to traditional voice telephony services, it adopted a more nuanced approach in 2004. In its Staff Working Document of June 2004,[63] the Commission explained that VoIP providers are subject to different rights and obligations under the Electronic Communications Regulatory Framework depending on whether they fall under the classification of "electronic communications service" (ECS)[64] or "publicly available telephone service" (PATS).[65] One of the aspects where VoIP differs from a traditional telephone service is the fact that users can be nomadic and use their terminal device at different locations. This had given rise to a number of new issues in relation to the provision of emergency services, and the Staff Working Document called on market players to work together to find solutions.

3–035 ***ERG common position on VoIP***—In December 2007, the European Regulators Group (ERG) adopted a common position on VoIP. The common position addressed the definitions used in the Electronic Communications Regulatory Framework, access to emergency services, numbering and number portability, and cross-border issues. The ERG urged the Commission to review the definitions for electronic communications in the context of the review of the Electronic Communications Regulatory Framework, and, for the purposes of the common position, introduced a new term, "telephony service", which would be subject to a common set of rights and obligations for both voice services over the public switched telephone network (PSTN) and VoIP. In its common position, the ERG took the position that all VoIP providers that offer outgoing calls to the PSTN would be required to offer access to the emergency services.[66]

3–036 ***VoIP under the revised Framework Directive*** —The revised Framework Directive partly follows the ERG's recommendations. It does not change the definition of ECS, but redefines "public communications network" (PCN) as "an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points."[67] At the same time, the revised Universal Service Directive redefines PATS as "a service made available to the public for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan."[68] Through the redefinition of PATS and PCN, the categories of service providers who are required to guarantee certain consumer rights, in particular under Articles 20, 21, 22, 23, 25 and 26 of the

numbering plan set out in the International Telecommunications Union's ITU-T Recommendation E.164): ERG Common Position on VoIP (ERG (07) 56rev2, December, 6–7, 2007. See para.1–317, above.

[62] European Commission, Notice of January 10, 1998 concerning the status of voice communications on the internet under EU law, and, in particular, pursuant to Directive 90/388, O.J. 1998 C6/4, updates by Commission (EC), Communication of December 22, 2000 on the status of voice on the internet under EU law, and, in particular, under Directive 90/388, O.J. 2000 C369/3.

[63] European Commission, Commission Staff Working Document of June 14, 2004, on the treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework—An information and Consultation Document, available at *http://ec.europa.eu/information_society/policy/ecomm/library/working_docs/index_en.htm*.

[64] Framework Directive, para.3–021, n.22, Art.2(c).

[65] Universal Service Directive, para.3–023, n.38, Art.2(c).

[66] At that time, VoIP providers under the classification of "electronic communications service" did not have this obligation, although some already offered emergency calls on a voluntary basis.

[67] Framework Directive, para.3–021, n.22, Art.2(d).

[68] Universal Service Directive, para.3–023, n.38, Art.2(c).

Universal Service Directive, have been modified in order to take into account IP-based services.[69] Access to emergency services, for example, must now be provided by all undertakings providing end-users with an electronic communications service for originating national calls to a number or numbers in a national telephone numbering plan.[70]

2. Free movement of internet services across the EU

3–037 **Free movement of services**—Under Article 56 TFEU [ex 49], service providers established in one Member State are free to provide services across the EU.[71] This provision is fully applicable to internet-based services. As a result, ISPs established in one Member State are free to provide services to customers located in another Member State. Article 56 TFEU requires Member States to refrain from introducing or maintaining any rule that restricts this freedom. In particular, this provision prohibits any national regulation that discriminates against providers of internet services established in other Member States. An obvious example of discrimination would be a requirement for internet users to gain access to the internet only through ISPs established in a given Member State. Article 56 also prohibits national rules that apply without distinction to national service providers and service providers established in other Member States, when the effect of the national rules is to render more costly or to discourage the activities of foreign service providers.[72]

3–038 **Possible exceptions to the free movement of services**—Under Article 52 TFEU [ex 46], restrictions on the free movement of services may be permissible if they are justified on the grounds of public policy, public security or public health. Moreover, non-discriminatory restrictions imposed in the general interest may be lawful, even if their effect is to restrict the activities of foreign service providers.[73] Considerations of the general interest that the Court of Justice has accepted as justifying restrictions on the free movement of services have included: (i) the maintenance of social order;[74] (ii) the protection of consumers and workers;[75] and (iii) the supervision of compliance with professional ethics rules.[76] As a result, it would in principle be permissible for a Member State to rely on national rules prohibiting, for instance, the distribution of child pornography or the incitement of violence or racism, to prevent the distribution on the internet of such content. Likewise, Member States could in principle rely on national consumer protection rules (*e.g.* national laws prohibiting sales at loss) to prevent the distribution over the internet of services that infringe such rules. There are, however, limitations on the ability of Member States to rely upon such exceptions to the principle of free movement of services. First, exceptions to a fundamental principle of EU law must be interpreted strictly. For example, it is an established principle that the "public policy" exception can only be successfully relied upon by Member States where

[69] For the status of VoIP under the revised electronic communications regulatory framework, see para.1–317, above.

[70] Universal Service Directive, para.3–023, n.38, Art.26(2).

[71] See para.2–003 *et seq.*, above.

[72] See paras.2–004 and 2–006, above.

[73] Case C–52/79, *Procureur du Roi v Marc J.V.C. Debauve* [1980] E.C.R. 883; see also paras.2–005 and 2–007, above.

[74] See para.2–007, n.24, above.

[75] See para.2–007, n.25, above.

[76] See Joined Cases C–110/78 and C–111/78, *Ministère public and "Chambre syndicale des agents artistiques et impresarii de Belgique" ASBL v Willy van Wesemael* [1979] E.C.R. 35; Case C–76/90, *Manfred Säger v Dennemeyer & Co. Ltd* [1991] E.C.R. I-4221; and Case C–106/91, *Claus Ramrath v Ministre de la Justice, and l'Institut des réviseurs d'entreprises* [1992] E.C.R. I-3351.

there is a "real and sufficiently serious threat, affecting a basic interest of society".[77] Second, the national measures must be proportionate to the public interest considerations that they seek to protect and must be the least restrictive measures for attaining such objectives.[78] Third, these exceptions may not be relied upon when they are effectively protecting an economic interest. Fourth, by analogy with the situation in the broadcasting sector, the application of non-discriminatory restrictions to foreign services is only justified in the absence of legislation at the EU level, unless such legislation permits Member States to impose restrictions. For example, the E-Commerce Directive permits Member States to impose restrictions on ISPs from other Member States under certain specified conditions.[79]

3–039 Notification of restrictions resulting from national technical standards—A specific mechanism has been set up at the EU level in order to ensure that national technical standards and regulations do not unduly restrict the free provision of information society services, including internet services, across the EU. This mechanism, which is the result of the Transparency Directive,[80] extends to information society services a system of prior notification of technical standards and regulations, which was previously applicable only to goods.[81] The Transparency Directive requires any draft national rule which is specifically (and not implicitly or incidentally) aimed at regulating information society services to be notified to the European Commission (and thereby effectively also to the other Member States) before implementation and at a time when it is still possible to amend it according to the applicable national legislative procedure.[82] Failure to notify the proposed national rule in accordance with the Transparency Directive may cause the national measures in question to be unenforceable.[83] The adoption of the draft national rule must be suspended for three months following its notification to the Commission.[84] This suspension period provides an opportunity for the Commission and the other Member States to consider whether the proposed national measure could create obstacles to the free movement of services between Member States and whether coordinated action at the EU level would be preferable. If this is the case, the three-month suspension period may be extended for up to an additional 15 months, until the adoption of legislation at the EU level on the subject. National rules concerning (linear)

[77] Case C–30/77, *R v Bouchereau* [1977] E.C.R. 1999.

[78] See para.2–007 n.23, above. For example, it is doubtful that a national law could lawfully prohibit the diffusion over the internet of certain types of content that can be viewed by minors when technical devices permit filtering of such content by parents.

[79] See para.3–114 *et seq.*, below.

[80] Transparency Directive, para.3–022, n.28. For a detailed commentary, see Dumortier, "Directive 98/48/EC of the European Parliament and of the Council", in Büllesbach, Poullet and Prins (eds.), *Concise European IT Law* (2006), 481–524.

[81] For a discussion of the Transparency Directive and its background, see d'Acunto, "Le Mécanisme de Transparence Réglementaire en Matière de Services de la Société de l'Information Instauré par la Directive 98/48/CE" (1998) 4 *Revue du Marché Unique Européen* 59.

[82] The Commission's DG Enterprise maintains a searchable database of all notified national measures, available at: *http://europa.eu.int/comm/enterprise/tris/*.

[83] See Case C–194/94, *CIA Security International SA v Signalson SA and Securitel SPRL* [1996] E.C.R. I-2201.

[84] Member States may immediately adopt the national measure without complying with the suspension obligation for urgent reasons related to the protection of public health or safety, public policy, notably the protection of minors, or the protection of the security and the integrity of the financial system: Transparency Directive, para.3–039, n.80, Art.9(7). Such measures must still, however, be notified to the European Commission.

broadcasting and telecommunications (in the traditional sense) are not subject to this notification requirement.[85]

D. Intellectual property rights and the internet

1. Copyright

3–040 Introduction—The ready availability on the internet of works protected by copyright constitutes a real challenge to the enforcement of copyright law. The open network nature of the internet, combined with digitisation, enables the production at low cost of copies of equivalent quality to the original of the work. In particular, the possibility for users to access and copy works placed on the internet from anywhere in the world makes enforcement of national copyright laws, whose territorial scope is limited, against infringers (both domestic and foreign) very difficult. The protection of copyright on the internet therefore raises many legal issues,[86] including: the determination of the types of work that can be protected by copyright (*e.g.* email, websites, computer programs, databases); the scope of copyright protection (*i.e.* moral and economic rights); and the exceptions to copyright protection (*e.g.* the ability to reproduce copyright works). The EU has adopted regulatory initiatives to address these issues.[87] Legislative action at the EU level has been motivated by the perception that the maintenance of divergent national copyright rules gave rise to legal uncertainty, thereby jeopardising the proper development of the information society, especially e-commerce, in Europe. In particular, the lack of adequate protection for works in digital form in certain Member States was considered an obstacle to the development of new products and services. The European Commission therefore recognised the need to ensure an appropriate level of copyright protection across Europe for works on the internet, which has to be achieved by the harmonisation of national provisions.

3–041 Scope of the Information Society Copyright Directive—The horizontal Information Society Copyright Directive[88] focuses on four aspects of copyright protection in respect of

[85] Transparency Directive, para.3–022, n.28, Annex V. In contrast to rules applying to traditional broadcasting services, national rules on non-linear audiovisual media services (such as video-on-demand) would fall within the regime established by the Transparency Directive in so far as such non-linear services would qualify as an information society service. On the notions of linear and non-linear audiovisual media services and the relation with information society services, see further, para.2–022 *et seq.*, above.

[86] For a detailed review of these issues, see Hance, para.3–001, n.1, 81–100; and Torremans, *Copyright Law: A Handbook of Contemporary Research* (Edward Elgar, 2007). The following section does not discuss the issue of secondary liability for copyright infringements, particularly peer-to-peer file sharing and online infringements: see Strowel, *Peer-to-Peer File Sharing and Secondary Liability in Copyright Law* (2009).

[87] For a discussion of other copyright directives, see para.2–149 *et seq.*, above.

[88] Directive 2001/29 of May 22, 2001 on the harmonisation of certain aspects of copyright and related rights in the Information Society, O.J. 2001 L167/10 ("Information Society Copyright Directive"). The Information Society Copyright Directive harmonises aspects of copyright in a horizontal way; in contrast to the existing copyright framework which always addressed these aspects in a vertical way. The Directive also served to implement the EU's and the Member States' obligations under the WIPO Copyright Treaty and the WIPO Performances and Phonogram Treaty, which deal with the protection of authors and the protection of performers and phonogram producers, respectively. In particular, the WIPO Copyright Treaty improves the means to fight worldwide piracy by providing authors with a cause of action against unauthorised circumvention of technical protection devices and the alteration of copyright management information. For a discussion of the WIPO Treaties, see Ficsor, *The Law of Copyright and the Internet: The 1996 WIPO Treaties,*

information society activities within the internal market: the reproduction right; the right of communication to the public; the distribution right; and the protection of technical measures and rights-management information. The Information Society Copyright Directive[89] does not affect, but rather complements, other EU copyright directives relating to: (i) the legal protection of computer programs;[90] (ii) rental rights, lending rights and certain rights related to copyright in the field of intellectual property;[91] (iii) copyright and related rights applicable to broadcasting of programmes by satellite and cable retransmission;[92] (iv) the term of protection of copyright and certain related rights;[93] (v) the legal protection of databases;[94] (vi) the resale right: and (vii) the enforcement of intellectual property rights.[95] Furthermore the Information Society Copyright Directive is without prejudice to other legal provisions, including in relation to patent rights, trade marks, design rights, utility models, semi-conductor topographies, type faces, conditional access services, access of broadcasters to networks, the protection of national measures, competition and unfair competition laws, trade secrets, security, confidentiality, data protection and privacy, access to public documents and contract law.[96] To the extent it has a horizontal dimension, the issue of liability for copyright infringement is not addressed in the Information Society Copyright Directive, but rather in the E-Commerce Directive and the Enforcement Directive.[97] The reference to the information society does not imply that its scope of application is limited to the internet: it also applies to traditional areas of copyright.

Their Interpretation and Implementation (2002). In many respects, the Information Society Copyright Directive goes well beyond the international obligations of both Treaties, though it did not harmonise all aspects of copyright; for example moral rights are not dealt with.

[89] Information Society Copyright Directive, para.3–041, n.88, Art.1(2).

[90] Computer programs obtain legal protection under Council Directive 91/250 of May 14, 1991 on the legal protection of computer programs, O.J. 1991 L122/42, as amended by Directive 93/98 of October 29, 1993, O.J. 1993 L290/9 ("Computer Programs Directive"). Computer programs that are available on the internet are already protected by copyright, pursuant to the Computer Programs Directive, provided that they are original in the sense that they are the author's own intellectual creation. As a result, the copyright owner of a computer program has the exclusive right to authorise the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole. Unless provided otherwise by contract, authorisation of the author would not be required for the reproduction of a computer program, where this reproduction is necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including error correction. This would cover permanent or temporary storage of a computer program on the user's computer hard disk if this is necessary to use a computer program acquired online. As discussed below, the Information Society Copyright Directive extends a similar principle beyond computer programs to cover any type of copyright work.

[91] See para.2–150 *et seq.*, above.

[92] See para.2–162 *et seq.*, above.

[93] See para.2–161., above.

[94] See para.3–060 *et seq.*, below.

[95] See para.2–172 *et seq.*, above.

[96] Information Society Copyright Directive, para.3–041, n.88, Art.9.

[97] An example of this would be an ISP's potential liability for contributory infringement of copyrights by permitting users to use their services or their network for the unauthorised transmission of copyright content. The issue was also considered by the Court of Justice in Case C-275/06, *Promusicae v Telefónica* [2008] E.C.R. I-271: see Coudert and Werkers, "In The Aftermath of the Promusicae Case: How to Strike the Balance?", (2010) 18 *International Journal of Law and Information Technology*, 50–71 and Kuner, "Data Protection and rights protection on the internet: the Promusicae judgment of the European Court of Justice", 5 (2008) E.I.P.R. 199–202. See also para.2–181, above.

3–042 ***Exclusive reproduction right***—Member States must provide for a copyright owner to have an exclusive right to authorise or prohibit the reproduction of his copyright work, whether a literary work, a fixation of a performance, a phonogram, a film or a broadcast. The reproduction right covers any direct or indirect, temporary or permanent reproduction by any means or in any form, in whole or in part of the copyright work.[98] This includes temporary copies made by the user's computer in order to enable use of the work.

3–043 *Exceptions to reproduction right*—An exception to the exclusive reproduction right is provided for temporary acts of reproduction that are (i) transient or incidental; (ii) are an integral and essential part of a technological process; (iii) have the sole purpose of enabling either the transmission of a work by an intermediary or the lawful use of a work or other subject-matter; and (iv) have no independent economic significance or value.[99] The exception covers acts of caching and browsing.[100] This exception has been criticised as being unprecedented in any copyright legislation and as being completely unclear.[101] Its purpose appears to be to exclude from liability for copyright infringement online service providers and other intermediaries who may unknowingly cache, host or transmit material that would otherwise infringe the reproduction right. Some commentators take the view that, rather than providing an exception, it defines the scope of the reproduction right.[102] In *Infopaq International*, the Court of Justice evaluated the concept of reproduction and the conditions that must be satisfied for the application of an exemption for temporary acts of reproduction as prescribed by the Information Society Copyright Directive. The Court held that the automated scanning and conversion into digital files of newspaper articles, followed by electronic processing of those files, was an act of "reproduction" within the meaning of Article 2 of the Information Society Copyright Directive. Therefore, as the storing of an extract of a protected work comprising 11 words and printing out that extract during a data capture process was not transient in nature (as required by Article 5(1) of Information Society Copyright Directive), that process could not be carried out without the consent of the relevant right holders.[103] In the *Copiepresse* case, the Brussels Court of First Instance held that the copy of a webpage stored in the memory of Google's servers and the display of a link making the cached copy accessible to the public infringed the reproduction and making available rights.[104] The exception is only applicable

[98] Information Society Copyright Directive, para.3–041, n.88, Art.2.

[99] *ibid.*, Art.5(1).

[100] *ibid.*, recital 33. "Caching" refers to the storage of frequently used information in areas more easily accessible to the user. ISPs may store cached material on servers that are in closer proximity to users' computers or on ones that receive less traffic, or even on users' hard disks. Caching involves copying all, or a substantial part, of the contents of a given web page: see Chissick and Kelman, para.3–005, n.9. "Browsing" is the act of searching the internet to locate or acquire information without knowing of the existence or format of the information sought: see *http://www.atis.org/tg2k/_browsing.html*.

[101] The EU Committee of the American Chamber of Commerce in Belgium, *EU Information Society Guide* (1998), 25; and Ross, "The Future of E.U. Copyright Law: the Amended Proposal for a Directive on Copyright and Related Rights in the Information Society" (1999) 4(4) *Communications Law* 128.

[102] Hugenholtz, *et al.*, *Final Report. The recasting of copyright and related rights for the knowledge economy, Study for the European Commission (DG Internal Market)* (November 2006), available at: *http://www.ivir.nl/publications/other/IViR_Recast_Final_Report_2006.pdf*.

[103] Case C-5/08, *Infopaq International A/S v Danske Dagblades Forening*, O.J. 2009 L220/7.

[104] Brussels Court of First Instance, February 13, 2007, *Google v Copiepresse*, (2007) 1–2 *Auteurs & Media* 107–122 (with case comment by Voorhoof), also available at: *http://www.droit-technologie.org/jurisprudence/details.asp?id=223*, with comment by Wéry, "Google News condamné par la justice belge pour violation de la loi sur les droits d'auteur", available at: *http://www.droit-technologie.org/actuality-1016/google-news-condamne-par-la-justice-belge-pour-violation-de-la-loi-sur.html*; appeal pending.

in certain specific cases that do not conflict with the normal exploitation of the work or other subject-matter, and that do not unreasonably prejudice the legitimate interests of the right holder.[105] The Information Society Copyright Directive contains an exhaustive list of other exceptions to the reproduction right, which Member States may choose (but are not required) to provide in their national copyright law, save the exception of the temporary reproduction contained in Article 5(1).[106] Given the broad margin of appreciation which is left to Member States, the harmonising effect of the Information Society Copyright Directive with regard to limitations is rather questionable.

3–044 *Grandfathering provisions for national limitations*—The Information Society Copyright Directive also includes a "grandfather" clause, which is somewhat inconsistent with the idea of the list being of an exhaustive nature. The grandfather clause refers to limitations which only apply in existing national copyright law and which only concern analogue uses. National limitations must not affect the free circulation of goods and services and only applies in cases of minor importance.[107] A recent European study points out there is a growing necessity for a multilateral instrument which can effectively harness various national practices with regard to exceptions and limitations to copyright and related rights, and which can provide a framework for the dynamic evaluation of how global copyright norms can be most effectively translated into a credible system that appropriately values authors' and users' rights.[108] The list of exceptions and national limitations includes: (i) reproduction (*i.e.* photocopying) on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects[109] (except for sheet music[110]); (ii) private copying on any medium by natural persons for non-commercial purposes;[111] (iii) reproduction for the sole purpose of illustration for teaching or scientific research; and (iv) reproductions of broadcasts by social institutions pursuing non-commercial

[105] Information Society Copyright Directive, para.3–041, n.88, Art.5(3).

[106] *ibid.*, Arts.5(2) to (5).

[107] *ibid.*, Art. 5(3)(o).

[108] Hugenholtz and Okediji, *Conceiving an international instrument on limitations and exceptions to copyright*, Study financed by the Open Society Institute, March 6, 2008, available at: *http://www.ivir.nl/publications/hugenholtz/limitations_exceptions_copyright.pdf*.

[109] It is not required that the reproduction is made by the person who ultimately benefits from the reproduction. Hence, copy shops offering services to persons who fulfil the conditions, may also benefit from the limitation.

[110] Music scores were left outside the scope of this exception, due to their widespread use in music circles and the lobbying efforts of music publishers.

[111] This exception covers reproduction by natural persons on both analogue and digital recording media. In the case of digital copying, the exception to the exclusive reproduction right is without prejudice to operational, reliable and effective technical means capable of protecting the interest of the copyright holder (*i.e.* technical means allowing copies to be tracked in order to ensure fair remuneration of the right holder). It would thus seem that, where operational and reliable copyright protection and royalty systems are in place, the exception would not apply: see Ross, para.3–043, n.101, 131. The Information Society Copyright Directive does not provide an enforceable right to private copying, but such an exception can be derived from both French and Belgian national case law: Brussels Court of Appeal, September 9, 2005, *Test Achats v EMI Recorded Music Belgium et al.*, (2005) 4 *Auteurs & Media* 301; (2005) 37 *Revue de Jurisprudence de Liège, Mons et Bruxelles* 1644; (2006) 28 *Journal des Tribunaux* 528; French Cour de Cassation, February 28, 2006, case No.549, *Studio Canal et al. v S Perquin and Union federale des consommateurs Que choisir*, (2006) *Bull.* I No.126, 115; (2006) 2 *Auteurs & Media* 177; Paris Court of Appeal, April 4, 2007, *Studio Canal et al. v S Perquin and Union federale des consommateurs Que choisir*, *Gazette du Palais*, July 18, 2007, No.199, 23.

purposes, in each case provided that the right holder receives fair remuneration.[112] Other exceptions, which are not specifically subject to the requirement that the right holders receive a fair compensation,[113] include: (i) reproductions made by publicly accessible libraries, educational establishments, museums or archives for non-commercial purposes; (ii) quotations from works that have already been made legally available; (iii) ephemeral recordings of works by broadcasters by means of their own facilities and for their own broadcasts;[114] (iv) use for teaching or scientific research;[115] (v) use for the benefit of people with disabilities for non-commercial purposes; (vi) reproduction by the press for reporting on current events;[116] and (vii) public security or use in administrative and judicial proceedings, etc. [117]

3–045 *Three-step test to apply exceptions and national limitations*—In addition to the specific conditions set out by the provisions regarding the exceptions, the Information Society Copyright Directive also contains a general limitation on the application of these exceptions and limitations, namely the internationally recognised three-step test.[118] According to this test, the exceptions should only apply in specific cases and cannot be interpreted in such a way as to allow their application in a manner that unreasonably prejudices the right holders' legitimate interests or that conflicts with the normal exploitation of their works or other subject matter.[119] It remains unclear whether the test is directed solely at Member States, when implementing the Information Society Copyright Directive, or can also be applied by national courts or the Court of Justice. According to many scholars, the European legislator wished to leave it to the Court of Justice to control the interpretation and implementation of the exceptions. Whether national courts, in addition to the Member States themselves, can apply the test will probably only become clear when the Court of Justice hands down a judgment on the matter.[120] The importance of the three-step test is not to be

[112] Information Society Copyright Directive, para.3–041, n.88, Arts.5(2) and (3).

[113] This notion was introduced by the drafters of the Directive in order to bridge the gap between the continental law states using levy systems (levies on blank media and reprographic equipment) and common law states which until now refused to introduce such a levy system. It should also be mentioned that DRM systems, enabling right holders to be compensated directly for particular uses, put into question further usage of levy systems: see *ibid.*, recital 35.

[114] When a broadcasting organisation is allowed to broadcast a work without the right holder's consent, this exception allows the broadcasting organisation to make the reproductions which are necessary in order to broadcast the work. A long term preservation of an ephemeral recording is only permissible if it is of exceptional documentary character and is preserved in an official archive. In order to be able to exploit the works in a later stage, a licence will have to be obtained: Dreier and Hugenholtz (eds.), *Concise European Copyright Law* (2006), 377.

[115] Recital 42 of the Information Society Copyright Directive further specifies that the non-commercial nature of the activity in question should be determined by that activity as such. The organisational structure and the means of funding of the establishment concerned are not the decisive factors in this respect.

[116] The Brussels Court of First Instance ruled that the mere grouping by Google News of fragments of published articles does not amount to reporting current events, due to the lack of any comment: *Google v Copiepresse*, para.3–043, n.104.

[117] Information Society Copyright Directive, para.3–041, n.88, Arts.5(2) and (3).

[118] Recognised at first by Art.9(2) of the Berne Convention, later adopted in Art.13 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Art.10 of the WIPO Copyright Treaty and Art.16 of the WIPO Performances and Phonograms Treaty. In contrast with these Treaties, the three-step test as set out by the Information Society Copyright Directive takes into account the interests of all right holders: authors, neighbouring right holders and licensees: see Senftleben, *Copyright, Limitations and the Three-Step Test—An Analysis of the Three-Step Test in International and EC Copyright Law* (2004), 82.

[119] Information Society Copyright Directive, para.3–041, n.88, recital 44.

[120] Hugenholtz *et al.*, para.3–043, n.102, 70.

underestimated, as it may considerably limit the application of the exceptions and hence have a deterrent effect on users from relying on an exception, since it may be declared illegal by a court. As a result of this legal uncertainty, users might feel obliged to seek the right holder's authorisation systematically. Some commentators stress the importance of a new interpretation of the three-step test in order to re-establish the balance between the interest of right holders and users.[121] The application of the three-step test leaves plenty of room for interpretation. However, the exception should only apply in special cases and must serve a specific public policy objective. The Information Society Copyright Directive should not be understood as requiring Member States to form special cases of the limitations listed in Articles 5(1) to 5(4) of the Directive. In addition, the exempted use should not conflict with the normal exploitation of the copyright work, which implies that the limitation should not deprive the right holder of general benefits. To determine what that exactly entails, it will be necessary to rely on economic studies. The exempted use may not unreasonably prejudice the right holder's legitimate interests: this refers to the fact that the exception may not unreasonably tip the balance between the interests of right holders and third parties. The (potential) prejudice should be evaluated both in quantitative and qualitative terms and the existence or non-existence of an equitable remuneration should also be taken into account.[122]

3–046 ***Exclusive right of communication of a work to the public***—Member States must provide authors with the exclusive right to authorise (or prohibit) any communication or making available to the public, by wire or wireless means, of the copyright work.[123] The right of communication to the public only covers communication to a public which is not present at the place at which the communication originates, *i.e.* broadcasting, cable, or online transmissions; it does not cover communication to the public at that place, *i.e.* recitation, display, public performance.[124] The Information Society Copyright Directive also provides for the right of communication to the public for holders of neighbouring rights, *i.e.* performers, phonogram producers, film producers and broadcasters, but only with respect to communications to members of the public that were not present at the time of the original performance, filming, etc., *e.g.* performers are ensured the right to control the subsequent, recorded communication of their performance. The Directive does not affect their rights in the original performance to the public, [125] as codified in Article 8 of the Rental Right Directive[126] and Article 4 of the Satellite and Cable Directive.[127] This seems to introduce an element of discrimination between copyright owners, *i.e.* authors of literary works (whose rights are protected regardless of the media) and holders of neighbouring rights.[128]

[121] See Geiger, "From Berne to national law, via the Copyright Directive: the dangerous mutations of the three-step test" (2007) E.I.P.R. 486–491; Koelman, "Fixing the three step test" (2006) E.I.P.R. 407–412; and Hugenholtz and Okediji, para.3–044, n.108, 25.

[122] Information Society Copyright Directive, para.3–041, n.88, Art.5(5); Dreier and Hugenholtz (eds.), para.3–044, n.114, 381–383.

[123] *ibid.*, Art.3.

[124] Dreier and Hugenholtz (eds.), para.3–044, n.114, 360.

[125] Information Society Copyright Directive, para.3–041, n.88, recital 24 and Art.3(2).

[126] Directive 2006/115 of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version), O.J. 2006, L376/28 ("Rental Right Directive"). See also para.2–150 *et seq.*, above.

[127] Council Directive 93/83/EEC of September 27, 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, O.J. 1993 L248/15 ("Satellite and Cable Directive"). See also para.2–162 *et seq.*, above.

[128] Ross, para.3–043, n.101, points out that the Rental Right Directive and the Satellite and Cable Directive do not provide holders of neighbouring rights with a right of communication to the public in non-interactive media to the same extent as that provided by the Information Society Copyright Directive to authors.

3–047 *Communication of works to the public*—The "communication" of works to the public covers the transmission or retransmission to the public by wire or wireless means, including broadcasting. However, the mere provision of physical facilities for enabling or making a communication does not amount in itself to an act of communicating a work to the public.[129] This excludes from the scope of the right of communication to the public, activities such as those of operators of telecommunications networks that are performed only in preparation of an act of communication of works and the making available of the subject-matter to the public. The "making available" right is a special case of the general right of communication to the public. The Information Society Copyright Directive specifies that the right of communication to the public includes the making available of works in such a way that members of the public may access them from a place and at a time individually chosen by them, *i.e.* when using online interactive on-demand services, including the internet and interactive digital television. The mere possibility of the public having access to the work suffices, *e.g.* by viewing a film on a pay-per-view TV channel. If a work is offered in such a way that a member of the public does not have individual control over when and where he wants to have access to the work (*i.e.* mere broadcasting, streaming content over the internet or near-on-demand pay-TV), the "making available" right does not apply, but the more general right of communication to the public will be applicable. Exceptions to the right of communication to the public include, amongst others, communication of works and the making available of other subject matter to the public for: (i) teaching or scientific research; (ii) current reporting of economic, political or religious topics;[130] (iii) quotations, for purposes such as criticism or review; (iv) the benefit of people with disabilities; (v) public security or use in administrative and judicial proceedings; and (vi) private research or study, to individual members of the public by dedicated terminals on the premises of libraries, education establishments or museums of works and other subject matter not subject to purchase or licensing terms that are contained in collections.[131]

3–048 ***Exclusive distribution right***—The Information Society Copyright Directive also requires Member States to provide authors with an exclusive distribution right, in respect of the works or copies thereof, to authorise (or prohibit) any form of distribution to the public by sale or otherwise.[132] The exclusive distribution right is attributed solely to authors.[133] It only covers the dissemination of fixations of works which can be put into circulation as tangible objects, not the transmission of works over non-tangible media, in particular online transmission.

3–049 *Exhaustion of distribution right*—The distribution right is exhausted by the first sale or other transfer of ownership (such as donation or exchange)[134] of the original of the work or a copy

[129] Information Society Copyright Directive, para.3–041, n.88, recital 27. The installation of physical facilities—such as television sets in hotel rooms—may nevertheless make public access to broadcast works technically possible. In that case, the distribution of the signal to customers staying in the hotel will constitute a communication to the public, irrespective of the technique used to transmit the signal: Case C-306/05, *SGAE v Rafael Hoteles SA* [2006] E.C.R. I-11519.

[130] The mere grouping of fragments of published articles, such as the Google News service, without comment, cannot benefit from this exception: *Google v Copiepresse*, para.3–043, n.104.

[131] Information Society Copyright Directive, para.3–041, n.88, Art.5(3).

[132] *ibid.*, Art.4(1).

[133] Distribution rights for related rights (fixations of performance, phonograms, films and broadcasts) were already provided for by Art.9 of the Rental Right Directive, para.3–046, n.126.

[134] There has to be a transfer of the *de facto* power of disposal. Merely exhibiting a reproduction of a work

thereof in the EU by the right holder or with his consent.[135] Exhaustion of the distribution right does not occur when the first sale takes place without the consent of the right holder, regardless of whether this occurs outside or within the EU, for example, as a result of a compulsory licence. Likewise, exhaustion does not arise in relation to works made available online, since the distribution of a work through online access alone should be analysed as the provision of a service rather than as the distribution of a copyright work.[136] The same analysis applies to a material copy of a work or other subject matter made by a user of such an online service with the consent of the right holder. Accordingly, every online service may be subject to authorisation where the copyright or related right so provides.[137] According to some scholars, the latter provision may also be interpreted in another way. It could be argued that exhaustion does take place with regard to a material copy made by the user with the right holder's consent, provided the user does not retain a dataset of the work after he has sold the material copy. Given the difficulties of proof, however, it could also be argued that the control interests of the right holder should still prevail.[138] Interpreting the concept of "consent" is not a matter of simply applying national laws, but of interpreting Article 4(2) of the Information Society Copyright Directive directly with respect to the similar consent requirement contained in Article 7(1) of the Trademark Directive.[139] Usually, consent will be granted in an express way, but it may also be inferred from facts or circumstances prior to, simultaneous with or subsequent to, the placing of the work on the market. The right holder cannot limit his consent in geographical terms, but may limit his consent to the distribution by a third party to a certain time frame, to a certain mode of distribution[140] or to particular copies of his work.[141]

3–050 *Exceptions to distribution right*—Member States may provide exceptions to the distribution right in those cases where they provide for exceptions to the reproduction right, so long as it is justified by the purpose of the authorised act of reproduction.[142]

3–051 ***Protection of technical measures to prevent copying***—Digitisation and especially the emergence of the internet have enabled mass-scale piracy and counterfeiting. Technological developments have allowed right holders to make use of technological measures to prevent and

in a shop display window, without making it available for use, does not constitute a form of distribution to the public: Case C-456/06, *Peek & Cloppenburg KG v Cassina S.p.A.* [2008] E.C.R. I-2731.

[135] On the exhaustion of rights doctrine as developed by the Court of Justice, see para.3–064, n.193, below; Information Society Copyright Directive, para.3–041, n.88, recital 28.

[136] Information Society Copyright Directive, para.3–041, n.88, recital 29. The Court of Justice has, on several occasions, confirmed that the principle of exhaustion does not apply to services, but only to the trading of tangible goods: Case 62/79, *Coditel v Ciné Vog Films and others (No.1)* [1980] E.C.R. 881; Case 262/81, *Coditel v Ciné Vog Films and others (No.2)* [1982] E.C.R. 3381; and Case 395/87, *Ministère Public v Tournier* [1989] E.C.R. 2521.

[137] Information Society Copyright Directive, para.3–041, n.88, recital 29.

[138] Dreier and Hugenholtz (eds.), para.3–044, n.114, 363.

[139] Joined Cases C-414 to 416/99, *Zion Davidoff v A & G Imports and others* [2001] E.C.R. I-8691; Directive 2008/95 of October 22, 2008 to approximate the laws of the Member States relating to trade marks (codified version), O.J. 2008 L299/25 ("Trademark Directive").

[140] In which case the question remains whether such limited consent also means that the effect of the exhaustion is limited to those specified types of distribution. The Information Society Copyright Directive is silent on this issue.

[141] Case C-173/98, *Sebago Inc. and Ancient Madison Dubois & Fills SA v G-B Runic S.A.* [1999] E.C.R. I-4103.

[142] Information Society Copyright Directive, para.3–041, n.88, Art.5(4).

inhibit the infringement of copyright and neighbouring rights.[143] In order to increase the protection of content distribution in the information society context, it was deemed necessary to develop a legal framework which prohibits the circumvention of various technological protection measures, as well as the production and distribution of devices which can be used to circumvent such measures. Some commentators fear that, as a consequence, the scope of copyright is no longer in accordance with what its proper scope should be, but in accordance with what the technology can do.[144]

3–052 *Scope of protection*—The Information Society Copyright Directive[145] requires Member States to provide adequate legal protection against the unauthorised circumvention of any effective technological measure designed to protect copyright and related rights (including the *sui generis* right provided by the Database Directive) that is carried out in the knowledge, or with reasonable grounds to know, that this objective is being pursued. [146] Technological protection measures can be digital or analogue; both are protected by the Information Society Copyright Directive. In practice, technological measures are often referred to as "DRM" (Digital Rights Management), which implies a more complex protection system using technological, contractual and statutory protection concurrently, whereas the term "technological measures" refers to simple, individual technologies.[147] In particular, Member States must also provide adequate legal protection against the manufacture, distribution,[148] sale, rental, advertisement for sale or rental,[149] or possession for commercial use of devices, products or components which are primarily designed, produced, adapted or performed for the purpose of facilitating the circumvention of any effective technological measures designed to protect copyright and related rights.[150] Adequate protection must also

[143] For a discussion of the different types of technological measures that can prevent unauthorised copying, see Marks and Turnbull, "Technical Protection Measures: The Intersection of Technology, Law and Commercial Practices" (2000) 22(5) E.I.P.R. 198. The two main forms of technological protection measures are access control and copy protection. Access control includes measures such as encryption. Access control devices can be installed on computer hardware. Copy protection devices control the copying of content, by incorporating bags in digital signals that must be recognised by hardware. Examples of copy control measures include serial copyright management system (SCAMS), which allows users to make an unlimited number of copies from the original, while preventing them from making copies of the copies, and the contents scramble system (CUSS), which was designed to prevent the copying of DVD films.

[144] Dussolier, "Technology as an imperative for regulating copyright: from the public exploitation to the private use of the work", (2005) E.I.P.R. 201.

[145] Information Society Copyright Directive, para.3–041, n.88, Art.6(1).

[146] *ibid.* Some commentators have argued that this provision may limit the ability of consumers to protect themselves from privacy-invasive technological measures: see, *e.g.*, Bygrave, "The Technologisation of Copyright: Implications for Privacy and Related Interests" (2002) 24(2) E.I.P.R. 51. Bygrave argues that devices such as cookies that are used to monitor private usage of copyrighted works for the purpose of detecting copyright infringements can be considered protected technological measures. Therefore, consumers' use of technological devices or software that interferes with their operation could amount to an infringement under the Information Society Copyright Directive.

[147] Dreier and Hugenholtz (eds.), para.3–044, n.114, 386.

[148] This covers both tangible circumvention tools, as well as the online transmission of circumvention tools.

[149] The Munich Court of Appeals has held that reporting on a news site regarding circumvention tools for commercial purposes could not be qualified as an advertisement within the meaning of Art.6(2). Moreover, the principle of press freedom was an issue in this case and the removal of the hyperlink to the company providing the tools was prohibited: Court of Appeals, Munich, Case U 2887/05, July 28, 2005 (2005) *Multimedia und Recht* 774, (2005) GRUR-RR 372.

[150] The private possession of circumvention tools can be forbidden by Member States: Information Society Copyright Directive, para.3–041, n.88, recital 49.

be provided against the provision of services, which are promoted, advertised or marketed for the purpose of circumvention, which have only a limited commercially significant purpose or use other than to circumvent.[151] A technological measure includes any technology, device or component that is designed to prevent or restrict unauthorised acts which are not authorised by the right holder. It is deemed to be effective if access to, or the use of, a protected work or other subject-matter is controlled through the application of an access code or any other type of protection process that achieves the protection objective in an operational and reliable manner with the authority of the right holder.[152] Such processes may include encryption, scrambling or other transformation of the work or other subject-matter. These provisions are without prejudice to the right to decompile a computer program in order to ensure interoperability with other computer programmes, as provided for by the Computer Programs Directive.[153]

3–053 *Exceptions and limitations*—According to Article 6(4) of the Information Society Copyright Directive, notwithstanding the prohibitions on the circumvention of technical measures to prevent unauthorised copying, Member States must take appropriate measures to ensure that right holders make available to the beneficiaries of certain exceptions and limitations the means of benefiting from these exceptions and limitations.[154] The covered exceptions and limitations are those applying to: (i) photocopies; (ii) copies made by libraries, educational establishments or museums; (iii) ephemeral recordings made by broadcasting organisations; (iv) reproductions of broadcasts by social institutions; (v) reproductions or communication to the public for the sole purpose of teaching or scientific research; (vi) reproductions or communication to the public for people with disabilities; and (vii) reproductions or communication to the public for public security or official use.[155]

3–054 *Voluntary facilitation of exceptions and limitations*—Right holders may make available such means by voluntarily adopting the necessary technological measures (which shall themselves enjoy protection from circumvention in order to prevent their abuse) or by entering into any necessary agreements. Technological measures applied voluntarily by right holders, including those applied in the implementation of a voluntary agreement, must enjoy legal protection.[156]

3–055 *Compulsory facilitation of exceptions and limitations*—If voluntary measures or agreements are not put in place within a reasonable period of time, Member States may also put in place measures to modify the technological measures taken by right holders to the extent that their

[151] Information Society Copyright Directive, para.3–041, n.88, Art.6(2). This implies, in practice, that systems which have lawful purposes as their main function, but that incidentally enable the circumvention of technological measures to prevent copying, fall outside of the scope of this provision: Ross, para.3–043, n.88, 132.

[152] Information Society Copyright Directive, para.3–041, n.88, Art.6(3). As such, the notion of "effectiveness" does not refer to whether significant or *de minimis* efforts were needed to circumvent the technological measure.

[153] *ibid.*, Art.6(4), fifth para. and recital 50. See also Computer Program Directive, para.3–041, n.90, Art.6.

[154] *ibid.*, Art.6(4). For a general discussion of Art.6(4) of the Information Society Copyright Directive and its interpretation, see Casellati, "The Evolution of Art.6(4) of the European Information Society Copyright Directive" (2001) 24 *Columbia-VLA Journal of Law and the Arts* 369.

[155] *ibid.*, Art.6(4), first sub-para. These exceptions are contained in Arts.5(2)(a), 2(c), 2(d), 2(e), 3(a), 3(b), and 3(e). The first four exceptions and/or limitations apply only to reproduction rights, while the remaining three apply to both reproduction and communication rights.

[156] *ibid.*, Art.6(4), third sub-para. Thus, circumvention tools provided by right holders to consumers for the purpose of accessing copyrighted works must enjoy legal protection.

technological measures do not allow for the enjoyment of these exceptions or limitations.[157] Member States may also take such measures to ensure the benefits of the private copying limitation, unless right holders have made reproduction possible to the extent necessary to benefit from this limitation.[158]

3–056 *Limitations on compulsory national measures to allow copying*—Member States' powers to require right holders to permit authorised copying are subject to three important limitations. First, these powers can only be exercised in respect of beneficiaries that already enjoy legal access to the protected work or subject matter. Second, Member States can only do so in the absence of voluntary technical measures or voluntary agreements by right holders. Finally, the exceptions and limitations do not apply to interactive, on-demand content that is made available to the public on agreed contractual terms.[159] Some commentators have argued that the impact of these provisions is to elevate contract law over copyright law, because these provisions allow right holders to contract out of these exceptions and limitations.[160] Legal uncertainty exists regarding the specific scope of this major exception. The work must be offered for on-demand access, as described by the making available right, covering all transmissions over the internet, as long as the user is able to initialize the transmission. As recital 53 of the Information Society Copyright Directive states, non-interactive transmissions over the internet (such as webcasting, web-radio and similar transmissions where the user is not able to choose the time of transmission) do not fall under this scope of this exception. Some European Commission officials have stated that the exception contained in Article 6(4) only applies to video on-demand and similar services, although, according to other commentators, this is not what the broad wording of the Article implies.[161] Such an interpretation could jeopardise the good intentions phrased in Article 6(4), since it encourages making works exclusively available on demand, using the internet as a primordial distribution channel.[162] On the other hand, Article 6(4) of the Information Society Copyright Directive permits the implementation of a wide variety of approaches to solve the tension between technological measures and copyright exceptions. The Directive does not specify whether the obligations under Article 6(4) should be enacted as a statutory provision, or whether compliance with such obligations could be sought in court or left to alternative dispute resolutions. Finally, the Directive leaves it to the Member States to determine what kind of obligations are imposed on right holders (*e.g.* making circumvention tools available, providing access to copies of the work, cooperation obligations, etc.). The consequence of the discretion given to the Member States is that there is considerable divergence in the national solutions that have been adopted.[163]

3–057 ***Protection of rights management information***—DRM systems also offer means to identify and manage content. They allow right holders to keep perfect track of which consumers may access and use their content, under what circumstances and for which purposes. The Information Society

[157] *ibid.*, recital 51.

[158] *ibid.*, Art.6(4), second sub-para. This measure does not prevent right holders from adopting adequate measures to limit the number of private copies. Moreover, right holders must under all circumstances receive a fair compensation: *ibid.*, recital 52.

[159] *ibid.*, Art.6(4), fourth sub-para. By contrast, the non-interactive provision of online content remains subject to these exceptions and limitations: *ibid.*, recital 53.

[160] See Casellati, para.3–053, n.154, 392–393.

[161] Dreier and Hugenholtz (eds.), para.3–044, n.114, 394.

[162] Dussolier, "Exceptions and technological measures in the European Copyright Directive of 2001—an empty promise" (2003) 1(34) *IIC* 62–75.

[163] Dreier and Hugenholtz (eds.), para.3–044, n.114, 391–392.

Copyright Directive provides legal protection to prevent the manipulation or removal of the metadata, which are used by DRM systems. Member States must provide for adequate legal sanctions against any person who knowingly and without authority (i) removes or alters any electronic rights-management information, or (ii) distributes, imports for distribution, broadcasting communication or makes available to the public works or other subject-matter protected under the Information Society Copyright Directive or the Database Directive from which electronic rights-management information has been removed or altered without authority.[164] The expression "rights-management information" means any information provided by right holders that identifies the protected work or subject-matter, the author or other right holders, or information about the terms and conditions of use of the work or other subject matter, and any numbers or codes that represent such information.[165] Examples of such information include digital watermarking (which places a unique code in the content that cannot be removed without damaging the content), digital fingerprinting (which creates a digital trail as pieces of content are copied each time) and encryption.[166]

3–058 ***Sanctions and remedies***—Member States must provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in the Information Society Copyright Directive and must take all measures necessary to ensure that those sanctions and remedies are applied.[167] Sanctions and remedies must be effective, proportionate and dissuasive. Member States must take measures necessary to ensure that right holders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material.[168] Injunctions should be obtainable against intermediaries (such as ISPs, including mere access providers)[169] whose services are used by a third party to infringe copyright or related rights, even if that intermediary benefits from an exception under Article 5 of the Information Society Copyright Directive:[170] the mere existence of a copyright infringement by a third party suffices.[171] Article 11 of

[164] Information Society Copyright Directive, para.3–041, n.88, Art.7, which also adds that the person should know or have reasonable grounds to know that by doing so he is inducing, enabling, facilitating or concealing an infringement of copyright, related rights or the *sui generis* database right.

[165] *ibid.*, Art.6(3). Due to privacy concerns, the protection given to rights management information does not apply to rights management information identifying consumers: *ibid.*, recital 57. Moreover, the scope of protection is limited to electronic rights management information; therefore, numbering systems such as ISBN, cannot benefit from the protection. On the other hand, the protection applies not only to rights management information, but also to machine-readable codes expressing this information, and neither is it necessary that the information is visible at all times for the consumer. Preparatory activities, which are prohibited under Art.6(2) with regard to technological protection measures, are not prohibited with regard to rights management information.

[166] Owen, "Digital Rights Management—Controlling Electronic Copying" (2002) 99 *In-House Lawyer* 28.

[167] Information Society Copyright Directive, para.3–041, n.88, Art.8(1).

[168] *ibid.*, Art.8(2).

[169] The Court of Justice has confirmed that: "An access provider offering users mere access to the internet—without providing other services such as news letter services, downloading and sharing of files and without exercising control both in fact or in law on the service being used—should be considered to be an intermediary in the sense of Article 8, paragraph 3 of Directive 2001/29": Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*, judgment of February 19, 2009, [2009] E.C.R. I-1227.

[170] Information Society Copyright Directive, para.3–041, n.88, recital 59 and Art.8(3), which consider that intermediaries are usually best placed to put infringing activities to an end.

[171] A Belgian court has even ordered an ISP to install software to exclude infringing peer-to-peer files in the future: Brussels Court of First Instance, *SABAM v Scarlet (ex-Tiscali)*, June 29, 2007, (2007) 5 *Auteurs &*

the Enforcement Directive does not affect Article 8(3) of the Information Society Copyright Directive.[172]

3–059 ***Implementation of the Information Society Copyright Directive***—Member States were required to implement the Information Society Copyright Directive by December 22, 2002. According to Article 10(1), the Directive applies to all works and other subject matter which were protected by the legislation of Member States on December 22, 2002. Article 10(2) further prescribes that the Directive shall apply without prejudice to any acts concluded and rights acquired before that date.[173] The wording "rights required" primarily concerns licence contracts in which right holders grant their exploitation rights to third parties. Also, it does not affect any contracts concluded or rights acquired prior to its entry into force, but applies to such contracts if those contracts had not expired before that date.

2. Legal protection of databases

3–060 **Background**—In the 1988 Green Paper on Copyright and the Challenge of Technology, the Commission had already indicated the need for better legal protection of databases and for the harmonisation of national rules in the EU.[174] As a result, the Database Directive was adopted on March 11, 1996 to harmonise national laws on the protection of databases.[175] Member States were required to implement the Database Directive into national law by January 1, 1998. In 2005, the European Commission published its first evaluation of the Database Directive.[176] The main purpose of this evaluation was to assess whether the policy goals of the Directive had been achieved and, in particular, whether the creation of a special *sui generis* right had had adverse effects on competition.[177] The Commission's report acknowledged that the Database Directive has not had any impact on the production of databases and suggested four policy options to address the regulation of databases.[178] These four policy options were the subject of a public consultation in 2006.[179] The Commission has, however, not taken any action since this time.

Media 476; (2007) 7 *Revue de Droit Commercial Belge* 701; (2008) 30 *Revue du Droit des Technologies de l'Information* 87; also available at: *http://www.droit-technologie.org/jurisprudence-233/sabam-c-tiscali-filtrage-des-contenus-p2p.html*. On January 28, 2010 the Court of Appeal of Brussels referred preliminary questions on the matter to the European Court of Justice (not yet reported). For commentary, see Verbiest and de Bellefroid, "Filtrage et responsabilité des prestataires techniques de l'internet: retour sur l'affaire SABAM c/ Tiscali" (2007) 246 *Légipresse* 156–160.

[172] Directive 2004/48 of April 29, 2004 on the enforcement of intellectual property rights, O.J. 2004 L157/45, *corr.* O.J. 2004 L195/16, recital 23 ("Enforcement Directive"): see para.2–172 *et seq.*, above.

[173] *ibid.*, Arts.10 and 13.

[174] COM(88) 172 final, August 23, 1998; see Derclaye, *The Legal Protection of Databases—A Comparative Analysis* (2008).

[175] Directive 96/9 of March 11, 1996 on the legal protection of databases (Database Directive), O.J. 1996 L77/20. For a more detailed review of the Database Directive, see, *e.g.*, Lehmann, "The European Database Directive and its Implementation into German Law" (1998) 29 (7) *ICC* 776–793.

[176] DG Internal Market and Services Working Paper, First Evaluation of Directive 96/9/EC on the legal protection of databases, December 12, 2005, available at: *http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf*.

[177] *ibid.*, 24.

[178] Option 1: repeal the whole Directive; option 2: withdraw the *sui generis* right; option 3: amend the *sui generis* provisions; and option 4: maintain the status quo: *ibid.*, 25–27.

[179] *ibid.*, 27. The list of contributions is available at: *http://circa.europa.eu/Public/irc/markt/markt_consultations/library?l=/copyright_neighbouring/database_consultation&vm=detailed&sb=Title*.

(a) Database Directive

3–061 The Database Directive applies to databases in both electronic and non-electronic form. A database is defined as "a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means".[180] This definition generally covers all commercially operated databases if they are equipped with a database (administration) system. However, the Database Directive does not apply to recordings; extracts from audio-visual, cinematographic, literary or musical works; or compilations of a number of recordings of musical performances on one phonogram, since the Database Directive was not intended to affect the protection granted to phonograms.[181] Multimedia anthologies with musical examples can, arguably, claim database protection.[182] The Database Directive does not apply to computer programs,[183] which are protected under the Computer Programs Directive.[184] The Database Directive established a dual regime of protection for databases: copyright protection for the structure of certain databases and a newly created *sui generis* right protecting the content of all databases.

(b) Copyright protection for databases

3–062 Conditions of eligibility—Databases are protected by copyright if, by reason of the selection or arrangement of their content, they constitute the author's own intellectual creation.[185] No other criteria shall be applied to determine the eligibility for that protection.[186] As a result, to qualify for protection, a database must not have been copied or plagiarised and the selection or arrangement of data must show a minimum of originality. The protection under the Database Directive applies to the structure of the database and does not extend to the contents of the database and is without prejudice to rights in the contents, including copyright protection, which will continue to be determined by the relevant provisions of national law and any relevant EU legislation .[187]

3–063 Beneficiaries of copyright protection for databases—Copyright rests in the author of a work. Authorship of a database belongs to the natural person or group of natural persons who created the database, or, when permitted by national law, to the legal person designated as the right holder by that legislation.[188] In contrast to the Computer Programs Directive,[189] the Database Directive does not provide for the transfer as a matter of law to an employer of the user rights relating to a database protected by copyright that is created by an employee in the execution of his duties or following the instructions given by his employer. However, Member States may provide for such a statutory transfer in their national legislation.[190]

[180] Database Directive, para.3–060, n.175, Art.1(2).
[181] *ibid.*, recital 17.
[182] Lehmann, para.3–060, n.175, 780.
[183] Database Directive, para.3–060, n.175, Art.2(b).
[184] *ibid.*, Art.2(a). See Computer Programs Directive, para.3–041, n.90.
[185] Database Directive, para.3–060, n.175, Art.3.
[186] *ibid.*
[187] *ibid.*, Art.3(2).
[188] *ibid.*, Art.4(1).
[189] Computer Programs Directive, para.3–041, n.90, Art.2(2).
[190] Database Directive, para.3–060, n.175, recital 29.

3–064 Scope of copyright protection for databases—The owner of copyright in a database benefits from all the rights generally granted by copyright protection:[191] (i) temporary or permanent reproduction by any means and in any form, in whole or in part; (ii) translation, adaption, arrangement or other alteration of the database; (iii) any form of distribution to the public of the database or of copies thereof; (iv) any communication, display or performance to the public; and (v) any reproduction, distribution, communication, display or performance to the public of any translation, adaptation, arrangement or other alteration. These very broad restricted rights would cover the temporary storage or transfer of a database on another medium, such that even browsing a database on the internet would be subject to the author's consent.[192] The author's exclusive right to any form of public distribution of a database or copies thereof in a physical form (*e.g.* on a CD-ROM) includes distribution in a non-physical form (*e.g.* online access). EU-wide exhaustion of the distribution right applies only to the first sale of each physical copy of a database: the author's rights are only exhausted in relation to that copy of the database and not the database generally.[193] The transfer of a database or part of it through online access alone should be analysed as the provision of a service, with the result that there is no exhaustion of rights.[194] This also applies with regard to a copy of all or part of an online database made by the user of online services with the consent of the right holder. Thus, there is no exhaustion of the distribution right in a database in the case of a permitted downloading and creation of a new copy and the author can prohibit any resale or further distribution of such a copy.[195]

3–065 Limitations on copyright protection—A lawful user of a database (*i.e.* a purchaser or a licensee) does not require the consent of the author for any of the restricted acts reserved to the author if they are necessary for the purposes of accessing the contents of the database and for normal use of the contents.[196] If the user is permitted to use only part of the database, this exception applies only to that part.[197] Any contractual provisions to the contrary are null and void.[198] Member States have the option of providing, under national implementing law, for limitations on the exclusive rights of the author in the following cases: (i) unrestricted reproduction for private purposes of a non-electronic database (*i.e.* databases whose elements are not individually accessible with the assistance of electronic means); (ii) use for the sole purpose of illustration for

[191] *ibid.*, Art.5.
[192] See Lehmann, para.3–060, n.175, 784. These provisions are without prejudice to the Information Society Copyright Directive, para.3–041, n.88, which stipulates that the temporary storage or browsing of any copyright content is subject to the author's consent, although it provides for an exception for temporary copies that enable the user to make use of the work, such as "caching": see para.2–171 and para.3–028 *et seq.*, above.
[193] Database Directive, para.3–060, n.175, Art.5(c). The "exhaustion of rights" principle, which results from the case law of the Court of Justice on the free movement of goods under Art.34 [ex 28] stipulates that an intellectual property right cannot be used to prohibit the sale in a Member State of goods which have been marketed in another Member State by the holder of the intellectual property right or with his consent. This principle was developed initially in relation to patents (Case–15/74, *Centrafarm BV et Adriaan de Peijper v Sterling Drug Inc.* [1974] E.C.R. 1147) and has gradually been extended to other intellectual property rights, including copyrights (Case–78/70, *Deutsche Grammophon Gesellschaft mbH v Metro-SB-Großmärkte GmbH & Co.* KG. [1971] E.C.R. 487).
[194] Database Directive, para.3–060, n.175, recital 33. See *Coditel v Ciné Vog Films (No.1)* and *Coditel v Ciné-Vog Films (No.2)*, para.3–049, n.136.
[195] Lehmann, para.3–060, n.175, 786.
[196] Database Directive, para.3–060, n.175, Art.6(1).
[197] *ibid.*
[198] *ibid.*, Art.15.

teaching or scientific research, provided the source is indicated and the extent of the reproduction is no more than justified by the non-commercial purpose to be achieved; (iii) where a database is used for the purposes of public security or for the purposes of an administrative or judicial procedure; and (iv) certain national exceptions to copyright traditionally authorised under national law.[199] These exceptions must not unreasonably prejudice the right holders' legitimate interests or conflict with the normal exploitation of the database.[200]

3–066 Term of copyright protection—Copyright in a database provides a EU-wide term of protection of 70 years, from the death of the author.[201] Where the author is a legal entity, the term of protection expires 70 years after the database is lawfully made available to the public.[202]

3–067 Remedies for infringement of copyright in a database—The Database Directive requires Member States to provide authors with appropriate remedies to enforce their rights under the Directive.[203] This gives Member States broad flexibility in this respect; remedies will ordinarily include damages, an account of profits from the infringement and injunctions.

(c) *Sui generis* database right

3–068 Conditions of eligibility—The main innovation of the Database Directive was to introduce a *sui generis* right, granting protection to database makers who have made a qualitative and/or quantitative substantial investment in the obtaining, verification or presentation of the contents of a database.[204] The *sui generis* protection applies regardless of whether the database or the content of the database show any of the intellectual creation needed for copyright protection and is also without prejudice to any rights existing in their contents. The *sui generis* right is a purely economic right, to protect the investment, deployment of financial resources and/or the time, effort and energy spent, in obtaining, verifying or presenting the contents of a database.[205] The concept of "investment" was considered by the Court of Justice in four judgments rendered in 2004.[206] According to the Court, the resources invested "in obtaining" the contents of a database refer to the resources used to find existing independent materials and collect them in the database,[207] while the resources invested "in the verification" refer to the resources used to ensure the reliability of the information contained in that database and to monitor the accuracy of the materials collected when the database was created and during its operation.[208] Neither the resources used for the creation of materials which make up the contents of a database, nor those used for verification

[199] *ibid.*, Art.6(2).
[200] *ibid.*, Art.6(3).
[201] Directive 2006/116 of December 12, 2006 on the term of protection of copyright and certain related rights, O.J. 2006 L372/12.
[202] *ibid.*, Art.1(4).
[203] Database Directive, para.3–060, n.175, Art.12.
[204] *ibid.*, Art.7(1).
[205] *ibid.*, recital 40.
[206] Case C-46/02, *Fixtures Marketing v Oy Veikkaus Ab* [2004] E.C.R. I-10365; Case C-203/02, *The British Horseracing Board v William Hill Organisation* [2004] E.C.R. I-10415; Case C-338/02, *Fixtures Marketing v Svenska Spel* [2004] E.C.R. I-10497; and Case C-444/02, *Fixtures Marketing v Organismos prognostikon agonon podosfairou AE—"OPAP"* [2004] E.C.R. I-10549. Each of these cases concerned databases of sports information (for either football or horseracing).
[207] *ibid.*
[208] *ibid.* See, in particular, *British Horseracing Board v William Hill Organisation*, para.3–068, n.206.

during the stage of creation of materials which are subsequently collected in a database, fall within those definitions.[209]

3–069 Beneficiaries of the *sui generis* protection of databases—The beneficiary of the *sui generis* protection is the "maker" of the database, which is the person who takes the initiative and the risk of investing in its creation.[210] This excludes contractors and employees from the protection. The *sui generis* right may be transferred or granted under contractual licence.[211] The *sui generis* protection of databases is only available to databases whose makers or right holders are nationals of Member States or persons who have their habitual residence in the EU.[212] It is also available to companies and firms formed in accordance with the laws of a Member State and having their registered office, central administration or principal place of business within the EU.[213] When such a company or firm has only its registered office in the EU, its operation must be genuinely linked on an ongoing basis with the economy of a Member State.[214] The possibility is provided for extending the benefit of the *sui generis* protection to databases made in third countries by way of international agreements concluded by the Council, upon a proposal from the Commission, provided that the term of protection does not exceed that granted to EU nationals, companies and firms.[215] Protection under the *sui generis* right granted by the Database Directive has been extended to citizens and companies of the EEA countries (*i.e.* Norway, Iceland and Liechtenstein)[216]. Proposals have been made at international level to adopt a global *sui generis* protection of databases.[217]

3–070 Scope of *sui generis* protection—The scope of the *sui generis* right is somewhat narrower than that of copyright. The holder of the *sui generis* right has the right to prohibit the extraction and/or re-utilisation of the whole or of a qualitatively or quantitatively substantial part of the contents of the database created by him.[218] Extraction involves the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form;[219] whilst re-utilisation covers any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by online or other forms of transmission.[220]

3–071 *Scope of extraction right*—The Court of Justice has held that the delimitation of the concepts of "permanent transfer" and "temporary transfer" is based on the criterion of the length of time during which materials extracted from a protected database are stored in a medium other than that database. The extraction of materials from a protected database that is accessible electronically occurs when the transferred materials are stored in a medium other than that database. The concept of extraction is independent of the objective pursued by the person performing the acts of extraction or transfer, any modifications that he may make to the contents of the transferred materials and any differences in the structural organisation of the database concerned.[221]

[209] *ibid.*
[210] Database Directive, para.3–060, n.175, recital 41.
[211] *ibid.*, Art.7(3).
[212] *ibid.*, Art.11(1).
[213] *ibid.*, Art.11(2).
[214] *ibid.*
[215] *ibid.*, Art.11(3).
[216] European Economic Area Agreement, Art.65(2), Annex XVII.
[217] Lehmann, para.3–060, n.175, 778.
[218] Database Directive, para.3–060, n.175, Art.7.
[219] *ibid.*, Art.7(2)(a).
[220] *ibid.*, Art.7(2)(b).
[221] Case C-545/07, *Apis-Hristovich EOOD v Lakorda AD*, O.J. 2009 C102/7.

The Court of Justice has also considered the scope of the extraction right: it has held that the "transfer" of material from a protected database to another database, following an on-screen consultation of the first database and an individual assessment of the material contained in that first database, is capable of constituting an extraction, to the extent either that (i) the operation amounts to the transfer of a substantial part of the contents of the protected database, or (ii) the transfers of insubstantial parts which, by their repeated or systematic nature, have resulted in the reconstruction of a substantial part of these contents of the protected database.[222] The expression "substantial part" is the critical element in determining the scope of both the *sui generis* right and acts which infringe it. The meaning of this term was clarified by the Court of Justice in *British Horseracing Board*.[223] According to the Court of Justice, the expression "substantial part" must be evaluated both from quantitative and qualitative perspectives. Quantitatively, it refers to the volume of data extracted from the database and/or re-utilised and assessed in relation to the total volume of the contents of the database; qualitatively, it points to the scale of the investment in the obtaining, verification or presentation of the contents of the data that has been extracted and/or re-utilised, regardless of whether that data represents a quantitatively substantial part of the general contents of the protected database. Any part which does not fulfil the definition of a substantial part, evaluated both quantitatively and qualitatively, constitutes an insubstantial part of the contents of a database.[224] EU-wide exhaustion of the *sui generis* right can only take place in relation to an individual copy of the database and occurs upon the first sale of that copy (*e.g.* on a CD-ROM).[225]

3–072 ***No exhaustion of rights***—There is no exhaustion of the maker's rights in the case of permitted online access to a database, even if the user is authorised to make a copy for himself. Article 7(5) of the Database Directive prohibits the repeated and systematic extraction and/or re-utilisation of substantial parts of the contents of a database, where this does not amount to a normal exploitation of the database or where such exploitation unreasonably prejudices the legitimate interests of the maker of the database: this would prevent a database being "abused" by a competitor over a prolonged period. [226]

3–073 **Limitations on *sui generis* protection**—The maker of a database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilising qualitatively or quantitatively insubstantial parts of its content for any purpose.[227] Any contractual provision to the contrary is null and void.[228] This limited user right would, for example, permit the citation of a database without the consent of the maker of the database. The exercise by a user of this right may not conflict with the normal exploitation of the database or unreasonably prejudice the legitimate interests of the maker of the database or the holders of

[222] Case C-304/07, *Directmedia Publishing GmbH v Albert-Ludwigs-Universität Freiburg* [2008] E.C.R I-7565; see also *Apis-Hristovich v Lakorda*, *ibid.* .

[223] *British Horseracing Board Ltd v William Hill Organisation*, para.3–068, n.206.

[224] *ibid.*

[225] Database Directive, para.3–060, n.175, Art.7. In relation to the application of the exhaustion of rights in respect of copyright, see para.3–049 *et seq.*, above.

[226] *ibid.* See also *British Horseracing Board v William Hill Organisation*, para.3–068, n.206: this prohibition refers to unauthorised acts of extraction or re-utilisation, the cumulative effect of which is to reconstitute and/or make available to the public, without the authorisation of the maker of the database, the whole or a substantial part of the contents of that database and thereby seriously prejudice the maker's investment.

[227] Database Directive, para.3–060, n.175, Art.8.

[228] *ibid.*, Art.15.

copyright and neighbouring rights in the works or the subject matter of the database.[229] As with copyright in databases, Member States have the option of providing, under national law, for limitations on the exclusive rights of the maker of the database, that will permit, without prior authorisation, the extraction or re-utilisation of a substantial part of a database in the following circumstances: (i) extraction for private purposes of a non-electronic database; (ii) extraction for the sole purpose of illustration for teaching or scientific research, provided that the source is indicated and the extent of the extraction is no more than is justified by the purpose of the teaching or research; and (iii) extraction and re-utilisation for the purposes of public security or for the purposes of an administrative or judicial procedure.[230]

3–074 **Term of protection under the *sui generis* right**—The protection of a database under the *sui generis* right runs from the date of the completion of the making of the database and expires 15 years from the first of January of the year following the date of completion.[231] However, any substantial change, evaluated either qualitatively or quantitatively, within that period to the content of a database results in a new 15 year term of protection for the *sui generis* right, provided that this involves a substantial new investment.[232] The burden of proof that the criteria are met for concluding that a substantial modification of the contents of a database is to be regarded as a substantial new investment lies with the maker of the database.[233] In practice, this results in unlimited protection for those databases that are updated regularly by way of successive additions, deletions or alterations.

3–075 **Remedies for infringement of the *sui generis* right**—As with copyright in databases, Member States have broad discretion in determining the adequate remedies to enforce *sui generis* rights.[234] In a number of Member States (*e.g.* Germany), the remedies are identical for infringement of copyright and the *sui generis* right.

3. Hypertext linking liability

3–076 **Hypertext linking**—Hypertext linking is the process whereby the user of one website is able to, by the click of the mouse, move between pages in the same site or to pages in another site. Hypertext links to other sites may either be initial links (which link to the home page of the second site) or deep links (which by-pass the home page of the second site and take users directly to internal pages). While the use of initial links between websites appears to be permissible, website owners are increasingly challenging the practice of deep linking, alleging that this practice violates their copyright, trademarks and database rights.[235] This issue is of particular relevance to search

[229] *ibid.*, Art.8(2).

[230] *ibid.*, Art.9.

[231] *ibid.*, Art.10.

[232] *ibid.*

[233] *ibid.*, recital 54.

[234] *ibid.*, Art.12; see para.3–065, above.

[235] Website owners have also put forward a number of other theories to object to hypertext linking, including: cable retransmission rights (United Kingdom), *Shetland Times Ltd v Dr Jonathan Wills* 1997 F.S.R. 604 (newspaper obtained injunction preventing another newspaper from linking to its news articles, because the articles were found to be a cable transmission); trespass (United States) *eBay v Bidders Edge* (2001) *E.C.L.R.* 12 (use of spiders by defendant to gather information on bids and displaying them on its website constituted a trespass because spiders used up so much of eBay's servers' capacity that they could not perform essential functions); and tortious interference with prospective business advantage (United States), *Ticketmaster v Tickets.com* (2001) *E.C.L.R.* 14 (Ticketmaster alleged that deep linking deprived it of advertising revenue; the

engines, which may infringe other's intellectual property rights by deep linking to the part of the website most relevant to the search, rather than the home page,[236] arguably depriving website owners of advertising or subscription revenue. A practice closely related to deep linking is "framing", which occurs when a click on the link from one site to another site brings up the second page "framed" within the original site. Some website owners have successfully argued that "framing" obscures the origin of the information contained in the second website and thus constitutes trademark infringement and/or unfair competition.[237]

3–077 Websites and database rights—The Database Directive defines a database as a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.[238] The Database Directive grants to the maker of a database, if it has made a substantial investment in the obtaining, verification and/or presentation of the contents, the right to prevent the extraction and/or re-utilisation of the whole or a substantial part of the contents of the database.[239] Websites consist of a number of data files (which are themselves often independently copyright works) that are stored in a systematic way. Therefore, websites are generally considered to be within the scope of the definition of a "database"[240] contained in the Database Directive. Judgments of national courts have confirmed this interpretation and found that deep linking to another website can be an infringement of the database rights in the linked website, as they concern a qualitatively substantial part of the database.[241] To succeed, plaintiff website owners must establish that they have made a substantial investment in the creation of the database and that the defendant unfairly extracted a quantitatively substantial part

case settled out of court). For a thorough review of the relevant cases, see Sableman, "Link Law Revisited: Internet Linking at Five Years" (2001) 16 *Berkeley Technology Law Journal* 1273.

[236] Greenwood and Davis, "Database Right—Developing IP Protection for the Internet Age" (2002) 100 *In-House Lawyer* 2.

[237] See Joslove and Krylov, "Dangerous Liaisons—Liability in the European Union for hypertext linking and search engine services", (2005) 2 *Computer Law Review International* 33–39; and Paeman and Aalto, "Hyperlinking Liability in Europe: Precedent and Future" (2001) 1(8) *World E-Commerce & IP Report* 6.

[238] Database Directive, para.3–060, n.175, Art.1(2); see also paras.3–042 *et seq.*, below.

[239] *ibid.*, Art.6(1).

[240] See Auld, "The Legal Classification of Websites and Liability for Hypertext Links" (2001) 17(4) *C.L.S.R.* 254.

[241] In the United Kingdom, see *British Horseracing Board v William Hill*, February 9, 2001, (2002) *E.C.C.* 24 (issues referred to the Court of Justice by the English Court of Appeal: see para.3–068, n.206, above), where it was held that a "database" covers nearly all collections of data in searchable form, including the plaintiff's database containing information on racehorses, jockeys and trainers that was required by bookmakers. In Germany, see *Stepstone v Ofir.de*, Landgericht Köln, judgment 28 O 692/00 of February 28, 2001, where it was held that the defendant's job-search engine infringed Stepstone's database rights by deep linking to its job listings, which in the process obliterated Stepstone's advertising banners. However, see also, in France, *Stepstone France v Ofir France*, Commercial Court of Nanterre, judgment of November 8, 2000, which held that deep links to Stepstone France's job listings did not infringe Stepstone's database rights, because Ofir France did not provide any information about jobs except hyperlinks and because it did not obliterate Stepstone France's advertising banners. In 2002, a Danish court held that the company *Newsbooster* violated copyright and marketing law by deep linking to articles in Danish newspapers. In February 2006, the Danish Maritime and Commercial Court reached the opposite conclusion in *Home v Ofir*, holding that deep linking, crawling and the use of search engines are vital functions of the internet and do not infringe the Database Directive: see Mercado-Kierkegaard, "Clearing the legal barriers—Danish court upholds 'deep linking' in Home v Ofir", (2006) 22 *C.L.S.R.* 326–332.

of the database[242] or repeatedly unfairly extracted qualitatively substantial parts of it.[243]

3–078 Hypertext linking and copyright—Hypertext links can also be classified as either "normal links" or "embedded links".[244] A normal link is simply a reference to other documents already available on the web, *i.e.* a shortcut so that users do not have to type out the document's URL. Normal links do not create an extra copy of the work other than the one created in the user's computer's random access memory (RAM). An embedded link is an electronic process that is automatically activated when the web page is loaded. It is often used to call up images, text or video that are part of another website, but which appear on the screen as an embedded part of the first website. Normal links, which make temporary copies, fall within the scope of the exclusive reproduction right, but such copies are permitted under the Information Society Copyright Directive and do not constitute an infringement.[245] Similarly, the use of embedded links does not involve making copies on the part of the linking site. A temporary copy is made on the user's computer, so while there is no infringement of the reproduction right, this practice may still infringe the exclusive right of communication to the public.[246] The usage of links has given rise to very divergent interpretations by courts of different Member States. In order to exempt certain uses, such as linking, courts have often resorted to a teleological interpretation of the reproduction right. The German Supreme Court ruled that hyperlinking one webpage to another does not constitute a communication to the public.[247] The Erfurt Regional Court decided that using thumbnails to establish links would not give rise to liability, provided the work was posted on the internet by the right holder or with his consent.[248] The Swedish Supreme Court[249] concluded linking could be considered as a communication to the public.[250] A French court decided that providing hyperlinks on a website to other websites offering the free download of music albums in MP3 format constituted a reproduction, distribution and communication (*i.e.* making available) of unauthorised copies of protected works.[251] In the well-known *Copiepresse v Google* case, the Brussels Court of First Instance in held that the display by a search engine of a link making the cached copy accessible to the public infringed both the reproduction right and the making available right. The Court did not order Google to remove the cached copies from its website, but did order

[242] In the Netherlands, see *Algemeen Dagblad BV v Eureka Internetdiensten*, judgment of August 22, 2000, where the Rechtbank Rotterdam held that a newspaper's website was not a database, because obtaining the information did not involve a substantial investment by the newspaper.

[243] In the United Kingdom, see *British Horseracing Board v William Hill*, para.3–077, n.241, where it was held that the defendant's repeated taking of substantial amounts of data on a daily basis was qualitatively substantial, because this was the most commercially valuable information.

[244] For a comparison of the treatment of potential copyright liability for hypertext linking in the United States, the EU and various Member States, see Garrote, "Linking and Framing: A Comparative Law Approach" (2002) 24(4) E.I.P.R. 184.

[245] Information Society Copyright Directive, para.3–041, n.88, Arts.2 and 5(1).

[246] *ibid.*, Art.3.

[247] Bundesgerichtshof (Federal Supreme Court), Case I ZR 259/00 BGH 156, July 17, 2003, *Paperboy*. See, in the same sense, Court of First Instance, Rotterdam, 139609/KG ZA 00-846, August 22, 2000, *Algemeen Dagblad BV v Eureka Internetdiensten ("Kranten.com")*.

[248] Erfurt Regional Court, 3 O 1108/05, March 15, 2007, *Bildersuche Suchmaschine Haftung*.

[249] Swedish Supreme Court, Case No.B 413-00, June 15, 2005, *Dr. Record Kommanditbolag et al. v Tommy Anders Olsson*.

[250] Dreier and Hugenholtz (eds.), para.3–044, n.114, 361.

[251] Tribunal de Grande Instance de Saint-Etienne (Court of First Instance), Case No.3561/1999, judgement of December 6, 1999, *SCCP et. Al. v Roche et Battie*. See, in the same sense, Cour d'Appel de Aix-en-Provence, judgment of March 10, 2004, *Roland v Ministère Public e.a.*

the removal of the links to the cached copies.[252] In addition, the usage of hyperlinks may constitute an infringement of the moral rights of a right holder.[253]

3. Trademarks—domain name disputes

3–079 Cybersquatting, typosquatting and cybercloning—As the commercialisation of the internet in general, and e-commerce in particular, has expanded, internet addresses and domain names have become increasingly valuable. This has led to the development of practices such as cybersquatting, which occurs when a third party, in bad faith, registers as a domain name the business name or trademark of an existing company. A variation of cybersquatting is typosquatting, where a slightly different or erroneously spelled version of a trademark, trade name or company name (*e.g.* gooogle.com instead of google.com) is registered with the intention to harm the interests of a third party or with the aim of obtaining an illicit advantage. A similar practice is cybercloning, whereby a foreign company appropriates the brand name and business model of a competitor in a given country and then registers an identical or a similar domain name with that country's ccTLD in order to establish a copycat business in the local market. The latest problems which have occurred involve "domain name front running", which is described as an opportunity for a party to obtain some form of insider information regarding an internet user's preference for registering a domain name and to use this opportunity to pre-emptively register that domain name,[254] and "domain tasting", the practice of using the "add grace" period to register domain names in bulk to test their profitability.[255] Many large, international companies, as well as well-known individuals, have found themselves the victims of these practices. They have sought redress in national courts or through the arbitration system established by ICANN and the WIPO, which is described below.[256]

3–080 Domain name dispute settlement system—In order to resolve the rapidly growing number of domain name disputes, ICANN and the WIPO jointly developed the Uniform Domain Name Dispute Resolution Procedure (UDRP),[257] which was formally adopted on August 26, 1999. The .eu Top Level Domain Regulation also contains an Alternative Dispute Resolution (ADR) process.

3–081 ***Uniform Domain Name Dispute Resolution Procedure***—The UDRP has been adopted by ICANN-accredited registrars in all gTLDs (*i.e.* .aero, .asia, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and .travel).[258] Dispute proceedings arising from alleged abusive registrations of domain names (for example, cybersquatting) may be initiated by a holder of trademark rights. The UDRP is a policy between a registrar and its customer and is included in registration agreements for all ICANN-accredited registrars. It provides an expedited administrative procedure for disputes involving allegations of abusive registration, under which trademark owners submit their complaints to an approved dispute resolution provider. The registration of gTLDs can be challenged when (i) a domain name is identical, or confusingly similar, to a trademark or service mark in which the complainant has rights; (ii) the registrant has no rights or legitimate interests in respect of the domain name; and (iii) the domain name is being used in bad faith. Dispute panels are empowered to require registries either to cancel improperly obtained domain names or to require the transfer of the domain name in dispute to a successful complainant.[259]

3–082 ***Dispute resolution for .eu registrations***—Separate rules apply for .eu registrations, which have been possible since 2006. Similar to the ICANN-procedure, allegedly abusive .eu domain name registrations can be challenged in national courts, but can also be settled using the Alternative Dispute Resolution (ADR) process contained in .eu Top Level Domain Regulation.[260] This process is handled by the Prague-based Czech Arbitration Court, an independent body selected by EURid.[261] Its rulings are legally binding, unless a losing party chooses to appeal the decision through the courts of a Member State. The registration of an .eu domain name can be challenged when it has been registered for speculative or abusive purposes, namely when (i) the .eu domain name registered is identical or confusingly similar to a name in respect of which a right is recognised or established by national and/or EU law, and (ii) the holder of the domain name has no rights or legitimate interest in the name or has registered or is using it in bad faith.[262]

E. Protection of privacy and security

3–083 Introduction—One of the main technical challenges in ensuring the commercial development of the internet is preserving the confidentiality and security of commercial transactions taking place over the internet. Moreover, techniques such as encryption technologies are constantly undergoing further development to respond to this challenge. This section reviews the EU regulatory framework on network security and the protection of privacy in relation to communications on the internet.

[252] Brussels Court of First Instance, *Google v Copiepresse*, para.3–043, n.104.

[253] Court of First Instance Leeuwarden, Case No.60145 KG ZA 03-281, October 30, 2003, *Tweewielercentrum Blokker VOF v Batavus B.V.*; and Civil Court Liège, February 27, 2007, *Kroll v Demol* (2007) 38 *Journal des Tribunaux* 804.

[254] Report on Domain Name Front Running from the ICANN Security and Stability Advisory Committee, SAC 024, February 2008.

[255] GNSO Issues Report on domain name tasting (June 14, 2007). Measures were adopted at the 32nd ICANN Meeting in Paris on June 26, 2008.

[256] See Cortés Diéguez, "An analysis of the UDRP experience—Is it time for reform?" 24 (2008) *Computer Law & Security Report* 349–359; Chaudri, "Internet domain names and the interaction with intellectual property" (2008) 24 *Computer Law & Security Report* 360–365; Kitterman, "Strategies for Preventing International Trademark Disputes: What Every Business Doing E-commerce Should Know" (2002) 2(2) *World E-Commerce & IP Report* 12; and Lemanski-Valente and Majka, "Trademarks and ccTLDs in the European Union: What US Trademark Owners Should Know" (2001) 136 Supp. *(Domain Names) Trademark World* 4.

[257] See *http://www.icann.org/dndr/udrp/policy.htm.*

[258] See Bettink, "Domain Name Dispute Resolution under the UDRP: The First Two Years" (2002) 24(5) E.I.P.R. 244. For a more critical review of the UDRP, see Thornburg, "Fast, Cheap, and Out of Control: Lessons from the ICANN Dispute Resolution Process" (2002) 6 *Computer Law Review and Technology Journal* 89.

[259] The ICANN website provides a full-text, searchable database for all disputes resolved by a decision: see *http://www.icann.org/udrp/udrpdec.htm.*

[260] See para.3–019, n.21, above.

[261] See *http://www.adr.eu.*

[262] Regulation 874/2004, para.3–019, n.21, Art.21.

1. Protection of the privacy of internet communications

3–084 The internet potentially represents a serious threat to privacy, as it is an open network. This means that private communications on the internet can be intercepted and that confidential files stored in computers connected to the internet can be accessed and copied from anywhere in the world. Moreover, many activities on the internet, often unnoticed by internet users, leave tracks that reveal personal data that may be collected, analysed and used in a different context. For example, visiting a website reveals information on users' habits and tastes, which may be useful for marketing purposes. The expanding use of the internet therefore raises a number of legal issues in relation to the protection of privacy, including the right of public authorities to monitor communications on the internet to prevent crime, and the right of employers to monitor the electronic correspondence and internet use of their employees. The internet is considered as the most prominent public communications network and enables the delivery of a wide range of electronic communications services. Therefore, the privacy issues that arise with regard to the internet fall under the scope of application of the European framework on privacy and data protection in the electronic communications sector. This framework is analysed in Chapter I and the particular problems relating to the internet are examined in that chapter.[263]

2. Security of internet communications

3–085 Technical aspects of internet security—Cryptographic technologies are widely recognised as essential tools for ensuring the security of, and trust in, electronic communications. Two important applications of cryptography are digital encryption and digital signatures.[264]

3–086 ***Encryption***—Encryption is the transformation of data into a form that is unreadable by persons that do not possess the decryption key. The process of transforming data back into a readable form is called "decryption". The purpose of encryption is to ensure confidentiality, by keeping the information hidden from anyone for whom it is not intended. There are two types of encryption systems: symmetric and asymmetric systems.

3–087 *Symmetric encryption*—In a symmetric encryption system, a key is used both to encrypt and decrypt data. In order for symmetric encryption systems to remain secure, the parties involved must keep the encryption key secret after they have communicated it to each other. The level of security may be improved by changing the private key regularly. An example of this system is the Data Encryption Standard (DES) developed by the US government.

3–088 *Asymmetric encryption*—An asymmetric encryption system (also called a "public key cryptography system") involves the use of two keys, a private key and a public key, which are related in a complex way. The sender creates an encrypted electronic signature to a given message with his private key and communicates his public key to all those with whom he wants to communicate authentic messages. By using the sender's public key, the receiver can then decrypt the signature and verify whether the message has been "signed" with the corresponding private key.

[263] See para.1–361 *et seq.*, above and, in particular, with respect to the confidentiality of communications, paras.1–402 *et seq.*, above.

[264] See Communication from the Commission, "Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signatures and Encryption" ("Commission Cryptography Communication"), COM(97) 503, Annexes 1–3; Brazell, "Electronic Security: Encryption in the Real World" (1999) 24(3) E.I.P.R. 17; and Baker, "International Developments Affecting Digital Signatures" (1998) 32(4) *The International Lawyer* 963.

The public key can also be used to encrypt messages that only the holder of the private key can decrypt. Public keys are usually published and accessible to everyone. The use of two different keys makes this system more secure than a symmetric encryption system. The only security problem raised by asymmetric encryption systems is ensuring the authenticity of the public key and guaranteeing that a public key indeed comes from the user to whom it is purported to belong. For that purpose, trusted third parties called certification authorities have been created to issue certificates for the public keys attesting the link between the public key and its holder and publish these certificates in publicly available registers. Involving the third trusted party makes the exchanges of authentic messages possible between people who may be unknown to each other. The leading certification authority is VeriSign.

3–089 ***Digital signatures***—Digital signatures are used to prove the origin of data (authenticity) and verify whether data has been altered (integrity). Furthermore, they make possible to prove at a later time that the signatory has not repudiated his statements (non-repudiation). A digital signature is a string of data created for a given message by using the sender's private key. It is obtained by computing, with the help of software, a mathematical "digest" of the message to be signed. The digest is created by applying special algorithms known as "hash algorithms". The digital signature, like a hand-written signature, is unique and different every time, because the result of the computation will depend on the contents of the message. This digest will then be encrypted using the sender's private key. Thus, the private key is not used to encrypt the message, but only to encrypt the digital signature. The receiver will then use the sender's public key to decrypt the digital signature and user software to compute the digest and compare both computed digests. Even the smallest change in the data would result in two diverging digests and would be discovered immediately. This system therefore permits the origin of a message (through the complementarity of the key-pair) and its integrity (through the hashing function) to be ascertained.

3–090 EU regulation of cryptography—The use of cryptography is essential in solving a number of legal issues raised by the use of the internet. It is, therefore, an important factor in its development.[265] First, encryption can ensure the confidentiality of communications disseminated over open networks. In that sense, encryption may contribute to preventing the unauthorised interception of messages sent over the internet. Second, the use of techniques such as digital signatures can greatly reduce the legal uncertainty regarding the use of the internet for trade purposes, because they guarantee the authenticity and integrity of data. Finally, cryptography also permits the enforcement of copyright and other intellectual property rights and conditional access to broadcasting services, which otherwise would be substantially undermined by the use of digital technology on open networks. For these reasons, it was considered at the EU level that the use of cryptography should be encouraged in order to ensure a more secure environment and thereby contribute to the development of the internet for commercial purposes.[266] Moreover, whilst some Member States had already adopted legislation or intended to do so, action at the EU level was perceived as being necessary in order to avoid divergent national regulatory systems that would have restricted inter-state trade in encryption products.[267]

[265] For a review of the legal issues raised by cryptography, see Brazell, para.3–085, n.264, 17; Szafran, "Regulatory Issues Raised by Cryptography on the Internet" (1998) 3(2) *Communications Law* 38; and Berhhard, "How to Secure the Network: Mutual Trust and Encryption" (1998) 3 *International Business Law Journal* 317.

[266] Commission Cryptography Communication, para.3–085, n.264, 1.

[267] *ibid.*

3–091 ***Restrictions on the use of cryptography***—Historically, law enforcement agencies and national security services have been concerned that cryptography could be used to transmit illegal messages and help perpetuate criminal or terrorist activities.

3–092 *Wassenaar Arrangement*—Through the Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies,[268] a group of 28 countries apply export controls to encryption products. Under the Wassenaar Agreement, cryptography is considered as a "dual-use" good, *i.e.* a good that can be used both for military and civilian purposes.

3–093 *EU Dual-Use Regulation*—The Dual-Use Regulation,[269] which replaces an earlier regulation that contained substantial limits on both intra-EU trade and exports, entirely liberalises intra-EU trade in information security products, including encryption, except for certain specialised products. Furthermore, undertakings may obtain a Community General Export Authorisation for exports of such products to 10 countries; for exports to other countries, exporters must apply for General National Licences, which are valid only for exports to a particular country. In this area, Member States faced a dilemma. On the one hand, they want to promote the use of techniques ensuring the security and the confidentiality of the internet, while on the other hand, they want to ensure that these techniques are not used to pursue illegal activities. A compromise may be found by encouraging the use of key escrow and key recovery systems, which are encryption systems providing a backup decryption capability allowing authorised institutions, under certain conditions, to decrypt data using archived keys that are under the control of Trusted Third Parties (TTPs). In a key escrow system, a copy of the secret key is deposited with an authorised TTP. The key can also be split into two or more parts that are deposited with different TTPs. In a key recovery system, the private key would not be immediately placed into escrow and the encryption system would allow authorised organisations, such as licensed TTPs, to rebuild the private key upon request. After considering the adoption of specific measures regulating key escrow and key recovery schemes, the Commission has moved away from its initial plan to prepare EU legislation on this subject, out of concerns for the protection of privacy raised by such systems.[270]

3–094 **Electronic Signatures Directive**—On November 30, 1999, the Council and the European Parliament adopted the Electronic Signatures Directive in order to facilitate the use of electronic signatures and certain certification services in the internal market.[271] The Electronic Signatures Directive has two objectives: (i) to remove obstacles to the legal recognition of digital signatures by laying down harmonised criteria on the legal effects of digital signatures; and (ii) to avoid regulatory disparities within the EU concerning the use of cryptographic technologies. Member States were required to have implemented the provisions of the Electronic Signatures Directive into national law by July 19, 2001.

[268] The Wassenaar Arrangement, which was signed in July 1996, replaced the Treaty of the Coordinating Committee for Multilateral Export Controls (COCOM), an international organisation for the control of the export of strategic products and technologies to proscribed destinations. Member States were, to a large extent, NATO members but also included other countries such as Japan and Australia. The Wassenaar Arrangement contains essentially the same provisions as the COCOM Treaty. See Szafran, para.3–090, n.265, 44.

[269] Council Regulation 1334/2000 of June 22, 2000 setting up an EU regime for the control of exports of dual-use items and technologies, O.J. 2000 L159/1.

[270] See Szafran, para.3–090, n.265, 47.

[271] Directive 1999/93 of the Council of December 13, 1999 on an EU framework for electronic signatures ("Electronic Signatures Directive"), O.J. 2000 L13/12.

3–095 ***Provision of certification services***—Certification services involve the verification of electronic signatures, so that recipients can be assured that an electronic signature belongs to the purported author. Member States must ensure that certification service providers can offer services without being required to obtain prior authorisation.[272] Member States may nevertheless introduce or maintain voluntary accreditation schemes aimed at enhancing levels of certification-service provision, provided that the conditions related to such schemes are objective, transparent, proportionate and non-discriminatory.[273] Such schemes should promote the levels of trust, security and quality demanded by the market and should encourage best practice; however, adherence to such a scheme cannot be made mandatory by a Member State. Member States must ensure the establishment of a system that allows for effective supervision of certification-service providers, including the determination of conformity with the requirements of the Electronic Signatures Directive of secure devices used to create electronic signatures.[274] A Member State may not restrict the provision of certification services originating in another Member State in the fields covered by the Electronic Signatures Directive.[275] In addition, Member States must ensure that equipment used for the creation or verification of electronic signatures or electronic signature certification services can circulate freely within the EU.[276] Electronic signatures in the public sector (in fields such as public procurement, taxation, social security, health and legal matters) may be made subject to additional requirements, where this is justified by the specific characteristics of the application concerned. Any new, additional criteria must be proportionate, non-discriminatory, transparent and objective and must not constitute obstacles to the cross-border provision of services.[277]

3–096 ***Common criteria for certificates authenticating electronic signatures***—Although certificates may be used for a variety of functions and contain different pieces of information, the Electronic Signatures Directive focuses on the regulatory framework applicable to advanced electronic signatures based on "qualified certificates". A qualified certificate must meet the requirements specified in Annex I of the Electronic Signatures Directive[278] and be issued by a certification service provider that meets requirements listed in the Annex.

[272] *ibid.*, Art.3(1); a certification-service provider is any entity or a legal or natural person who issues certificates or provides other services related to electronic signatures: *ibid.*, Art.2(12).

[273] *ibid.*, Art.3(2).

[274] The conformity of secure signature-creation devices is to be checked against the criteria in Annex III of the Electronic Signatures Directive. Such devices must ensure that signature-creation data used to guarantee electronic signatures can occur only once, are kept secret, and cannot be derived, *ibid.*, Arts.3(3) and 3(4). These tasks may be undertaken by public or private bodies. In addition, signatures must be protected against forgery, the signature-creation devices must be able to protect reliably against unauthorised use, and devices must not alter the data to be signed or prevent such data being presented to the signatory prior to the signature. The Commission may publish generally recognised standards for electronic signature creation devices, *i.e.* hardware or software intended for use by certification-service providers for the provision of electronic signature services, or for the creation or verification of electronic signatures. Compliance with Annex III shall be presumed if these standards are used: *ibid.*, Art.3(5). A certificate is defined "as an electronic attestation which links signature-verification data to a person and confirms the identity of that person": *ibid.*, Art.2(9), and an electronic signature is defined as "data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication:" *ibid.*, Art.2(1).

[275] *ibid.*, Art.4(1).

[276] *ibid.*, Art.4(2).

[277] *ibid.*, Art.3(7).

[278] *ibid.*, Annex 1. These requirements include, *inter alia*, (i) the identification of the certification service

3–097 ***Legal effects of electronic signatures***—Member States must ensure that advanced electronic signatures based on a qualified certificate and that are created by a secure signature-creation device satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data.[279] Member States must also ensure that such electronic signatures are admissible as evidence in legal proceedings.[280] This means that electronic signatures must be treated in the law in the same way as hand-written signatures, thereby promoting the conclusion of contracts and other documents online. Member States must also respect the legal effectiveness of any private agreements between participants in a closed system under which they will accept electronic signatures from each other.[281]

3–098 ***Liability of certification service providers***—The Electronic Signatures Directive lays down rules requiring the Member States to establish a minimum regime for the liability of certification service providers in relation to electronic signatures that are based on qualified certificates that they issue. In particular, Member States must ensure that, under their national laws, a certification service provider is liable for damages caused to any person who has reasonably relied on a certificate issued by it as regards the accuracy of the information contained in the qualified certificate and for the assurance that the signatory held the private key corresponding to the public key mentioned in the certificate and that both keys can be used in a complementary manner.[282] The certification service provider will not be liable if it can prove that it has not acted negligently. Member States must also impose liability on certification service providers for losses suffered by any person who reasonably relies upon a qualified certificate if they have negligently failed to register the revocation of a certificate.[283] Certification service providers must be given the option of limiting the use of a certificate or providing for a limit on the value of transactions for which the certificate can be used, provided that these limitations are communicated to third parties.[284] The certification service provider may not be held liable for damages arising from use of a certificate that exceeds the usage limitations placed upon it. The provisions of Article 6 of the Electronic Signatures Directive on the liability of certification service providers are without prejudice to EU law on unfair terms in consumer contracts,[285] such that any limitations of liability imposed by a service provider in a consumer contract must meet the requirements of reasonableness in order to be enforceable.

3–099 ***Third country certification service providers***—Certificates issued by certification service providers established outside the EU must be recognised as legally equivalent to certificates issued by certification service providers established in the EU if: (i) the third country provider fulfils the requirements of the Electronic Signatures Directive and has been accredited under the voluntary accreditation scheme of a Member State; (ii) a Community certification service provider, in

provider and the Member State in which it is established; (ii) the name of the signatory (or a pseudonym, which must be identified as such); (iii) the codes or public keys used for purposes of verifying an electronic signature; (iv) an indication of the beginning and end of the period of validity of the certificate; and (v) limitations on the use of the certificate, including any limitations as to the value of transactions for which it may be used. A "qualified" certificate must also clearly indicate that it is being issued as a qualified certificate.

[279] *ibid.*, Art.5(1)(a).

[280] *ibid.*, Art.5(1).

[281] *ibid.*, recital 16.

[282] *ibid.*, Art.6(1).

[283] *ibid.*, Art.6(2).

[284] *ibid.*, Arts.6(3) and 6(4).

[285] Council Directive 93/15 of April 5, 1993 on unfair terms in consumer contracts, O.J. 1993 L95/29.

compliance with the Directive, guarantees the certificate issued by the third country provider; or (iii) the third country provider, or the certificate it has created, is recognised under a bilateral or multilateral agreement between the EU and third countries or international organisations.[286] In order to facilitate the provision of cross-border certification services with third countries and the legal recognition of advanced digital signatures, the Commission may propose measures for the implementation of international standards and agreements, and may, if mandated by the Council (acting by qualified majority), negotiate bilateral and multilateral agreements with third countries and international organisations.[287] If companies established in the EU experience market access difficulties in third countries, the Council may mandate that the Commission negotiate comparable rights for EU undertakings in those third countries.[288]

3–100 **Attacks against information systems**—Information systems have been subject to an exponentially increasing number of attacks in recent years. The most common forms of attack include: hackers trying to gain unauthorised access to systems in order to copy, modify or destroy data; "denial of service attacks", which attempt to overload web servers or ISPs by bombarding them with a large number of automatically generated messages; viruses; the use of "sniffers", which intercept communications; and "spoofing", *i.e.* identity theft for the purpose of misrepresentation or fraud.[289] In response, the Council adopted a Framework Decision on attacks against information systems in February 2005.[290]

3–101 ***Harmonisation of offences under national law***—The Framework Decision harmonises legislation in the EU for any offence committed against a computer infrastructure with the intention of destroying, modifying or altering the information stored on computers or networks of computers. The key definitions concern the approximation of Member States' criminal laws regarding serious attacks against information systems through illegal access to them, or by illegal interference with them or by aiding, abetting or attempting such acts.[291] Intent has to be proven; gross negligence or recklessness are not sufficient to impose liability. Member States are required to ensure that serious attacks against information systems (such as those of the types listed above) are punishable by effective, proportionate and dissuasive penalties, including a maximum term of imprisonment of at least one to three years,[292] in order to bring these offences within the scope of the European arrest warrant[293] and other instruments such as the Decision on money

[286] Electronic Signatures Directive, para.3–094, n.271, Art.7(1).

[287] *ibid.*, Art.7(2).

[288] *ibid.*, Art.8(3).

[289] See Communication from the Commission of June 6, 1991, "Network and Information Security: Proposal for a European Policy Approach", COM(01) 298 (Information Security Proposal).

[290] Council Framework Decision 2005/222/JHA of February 24, 2005 on attacks against information systems. O.J. 2005 L69/67.

[291] *ibid.*, Arts.3–5.

[292] *ibid.*, Art.6.

[293] Council Framework Decision 2002/584/JHA of June 13, 2002 on the European arrest warrant and the surrender procedures between Member States, O.J. 2002 L190/1. The European arrest warrant was required to be operational by December 31, 2003. Member States' courts must issue European arrest warrants with a view to the arrest or surrender by the Member States of a person suspected of committing a criminal offence, for the purpose of conducting a criminal prosecution or executing a custodial sentence or detention order: *ibid.*, Art.1 (1). Warrants may be issued in respect of offences punishable by the law of the issuing state by a maximum period of at least 12 months' imprisonment or detention: *ibid.*, Art.2(1). As the Framework Decision on the European arrest warrant requires a maximum penalty of at least 12 months' imprisonment, Member States will be able to use a European arrest warrant to more easily detain and prosecute those suspected of attacking or misusing information systems.

laundering.[294] Furthermore, Member States are required to increase the maximum term of imprisonment to a period of two to five years if there are aggravating circumstances, *i.e.* if: (i) the offence is committed within the framework of a criminal organisation; (ii) the offence has caused serious damage or has affected essential interests.[295] Penalties must be imposed upon any individuals or organisations that commit these offences.[296] Member States are required to establish their jurisdiction to prosecute offences that are: committed on that Member State's territory; committed by their nationals; or if the offence is committed for the benefit of a legal person established in the territory of that Member State.[297] Member States must ensure that their jurisdiction includes both cases where (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; and (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.[298] Hence, the Framework Decision covers not only offences affecting the Member States (regardless of the location of the offender), but also offences committed in their territory against information systems located in the territory of other Member States and third countries. These provisions will be particularly important given the international nature of "cyber attacks", which enable perpetrators in one country to attack information systems in another. Member States were required to implement the Framework Decision by March 16, 2007.[299]

3–102 ***EU powers in the domain of criminal law***—Together with a number of other decisions and directives, the Framework Decision is affected by the Court of Justice's judgment in *Commission v Council (Environmental Protection Offences Framework Decision)*, in which the Court clarified the distribution of powers in criminal matters between the first and third pillars.[300] The Commission, supported by the European Parliament, had asked the Court to annul a Council Framework Decision on the protection of the environment through criminal law. The Court of Justice held that the Decision had been adopted on the wrong legal basis. Its judgment clarifies that, in relation to environmental protection (which falls within the EU's competence), the EU legislature may take measures which relate to the criminal law of the Member States, when the application of effective, proportionate and dissuasive criminal penalties by the competent national authorities is an essential measure for combating serious environmental offences. This is the case, even though, as a general rule, criminal law does not fall within the EU's competence.

3–103 **ENISA**—In 2004, the European Network and Information Security Agency ("ENISA") was established.[301] ENISA's function is to advise and coordinate the activities of different actors in the information security field, both private and public. Its specific tasks include: collecting information to analyse current and emerging risks which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them; providing opinions and

[294] Council Framework Decision of June 26, 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of the intermediaries of and the proceeds of crime, O.J. 2001 L182/1.
[295] Council Framework Decision on attacks against information systems, para.3–100, n.290, Art.7.
[296] *ibid.*, Arts.8 and 9.
[297] *ibid.*, Art.10.
[298] *ibid.*
[299] *ibid.*, Art.12.
[300] Case C-176/03, *Commission v Council (Environmental Protection Offences Framework Decision)* [2005] E.C.R. I-7879.
[301] Regulation (EC) No.460/2004 of March 10, 2004 establishing the European Network and Information Security Agency, O.J. 2004 L77/1. For more information about ENISA, see *http://www.enisa.europa.eu.*

support for harmonised processes and procedures in the Member States; identification of the relevant standardisation needs; enabling the exchange of information on network and information security, including best practices, between all users; promoting security standards and certification schemes; awareness raising and promotion of risk assessment activities and interoperable risk management solutions; and contributing to cooperation between the EU and third countries on information security issues.[302] In order to ensure that all relevant interests are represented, ENISA's Management Board consists of one representative of each Member State, three representatives appointed by the Commission, as well as three non-voting representatives, proposed by the Commission and appointed by the Council, to represent the following groups: (i) the information and communication technologies industry; (ii) consumer groups; (iii) academic experts in network and information security.[303] The Management Board appoints the Executive Director, who shall be independent in the performance of his or her duties.[304] The Executive Director is selected on the basis of a list of candidates proposed by the Commission after an open competition following publication in the Official Journal of the European Union and elsewhere of a call for expressions of interest. The Executive Director establishes a Permanent Stakeholders Group, who represents the aforementioned three stakeholder groups.[305]

F. Regulation of illegal and harmful content

3–104 **Successive Community Action Plans on the safer use of the internet**—One of the main benefits of the internet is that it permits greater and easier access to a wide variety of content. However, the internet can also be used to carry a considerable amount of harmful or illegal content and as a vehicle for criminal activities. Whilst the benefits of the internet far outweigh its potential drawbacks, its use to distribute illegal or harmful content could hamper its development by creating resistance to its use, especially by children. Although the prevention of crime on the internet is still essentially a matter of national law, from the late 1990s onwards a consensus developed among the Member States that, in view of the international character and complexity of the challenges encountered, action at the EU level was needed. This action would ensure the coordination and convergence of measures between Member States to control harmful and illegal use of the internet, avoid distortions of competition, ensure legal certainty and stimulate co-operation in a number of areas.

3–105 ***Internet Action Safety Plan***—As a result of the Member States' consensus for action at the EU level, a Community Action Plan on promoting the safer use of the internet ("Internet Safety Action Plan") was adopted in 1999, covering the period until 2002.[306] The Internet Safety

[302] *ibid.*, Arts.1–3.
[303] *ibid.*, Art.6.
[304] *ibid.*, Arts.7 and 11.
[305] *ibid.*, Art.8.
[306] Decision 276/1999 of January 25, 1999 adopting a multi-annual EU action plan on promoting safer use of the internet by combating illegal and harmful content on global networks, O.J. 1999 L33/1. For background on the EU's action in this area, see Communication from the Commission on illegal and harmful content on the internet, COM(96) 487; the two reports of the Working Party, "Illegal and Harmful Content on the Internet"; Communication from the Commission, "Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services", COM(96) 483; Communication from the Commission, "Action Plan on promoting safe use of the Internet", COM(97) 582; Council Resolution on illegal and harmful content on the Internet, O.J. 1997 C70/1.

Action Plan had four main lines of action: (i) the promotion of self-regulation as a tool for creating a safer internet environment; (ii) the development of filtering and rating systems; (iii) the encouragement of awareness actions; and (iv) the adoption of support actions.[307] The Commission subsequently amended the Internet Safety Action Plan, extending it until 2004 and adapting its scope and implementation to take account of the lessons learned and the development of new technologies, such as interactive services.[308] The Internet Safety Action Plan was opened up to participation by the then candidate and accession countries. The follow-up Internet Safety Action Plan did not contain any new regulatory initiatives and generally sought to increase the effectiveness of the existing policy framework.

3–106 ***Safer Internet Plus Programme***—As the end date of the Internet Safety Action Plan approached, it was felt that the complexity of the issues dealt with by it and the multiplicity of the actors with which it was concerned, meant that a follow-up was necessary.[309] As a result, in 2005, the Safer Internet Plus Programme[310] was adopted, again to promote safer use of the internet and new technologies, and to protect the end-users, particularly children, from unwanted content.

3–107 *Key action items of 2005 programme*—Four key actions were identified: (i) the fight against illegal content, with a focus on hotlines; (ii) tackling unwanted and harmful content, with a focus on filtering and rating; (iii) promoting a safer online environment, with a focus on self-regulation; and (iv) awareness-raising. Co-financing projects that attempted to achieve one or more of these aims remained the conceptual basis of the Safer Internet Plus Programme. Half of the available budget was earmarked for raising awareness. The Programme was based on principles of continuity (taking account of lessons learnt and building on achievements of the previous Internet Safety Action Plan's initiatives) and enhancement (meeting new threats and ensuring European added-value).[311]

3–108 *Revisions for 2009 programme*—In April 2007, the actions carried out under the Safer Internet Plus Programme (2005–2008) were evaluated and found to be effective, although they had to be adapted in the light of new needs, resulting from the emergence of new technologies and

[307] See Communication from the Commission, "Follow-up to the Multiannual Community Action Plan on Promoting Safer Use of the Internet by combating illegal and harmful content on global networks", COM(02) 152. The Commission released a report evaluating the results of the eEurope Action Plan in February, 2002, in which it concluded that the eEurope Action Plan had been very successful in meeting the goals set at the Feira European Council of June 2002, for example: dramatic increases in the proportion of EU citizens connected to the internet (from 18.3% in March 2000 to 42.6% in November 2002); the successful adoption of several of the legislative measures described in this chapter such as the E-Commerce and Digital Signatures Directive; increasing competition and lowering prices of internet access; increasing use of e-commerce; and increasing level of internet security. See Communication from the Commission, "eEurope 2002 Final Report", COM(03) 66.

[308] Decision 1151/2003 of June 16, 2003, amending Decision 276/1999 adopting a Multiannual Community Action Plan on promoting safer use of the internet by combating illegal and harmful content on global networks, O.J. 2003 L162/1.

[309] Proposal for a Decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies, COM (2004) 91 final, 2.

[310] Decision 854/2005 of May, 5, 2005, establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies, O.J. 2005 L149/1.

[311] Proposal for a Decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies, COM (2004) 91 final, 6. See also Decision 854/2005 of the European Parliament and of the Council, para.3–106, n.310, recital 6.

services.[312] Consequently, a follow-up programme appeared justified and a proposal for the extension of the Safer Internet Plus Programme from 2009 until 2013 was proposed by the Commission.[313] The proposal aimed to provide practical help for the end-user (*e.g.* children, parents, carers and educators), and sought to involve and bring together the different stakeholders whose cooperation is essential. The scope of the programme was extended, to focus on grooming and cyberbullying and to provide more knowledge on the ways children use new technologies. Four lines of action were again identified: (i) ensuring public awareness; (ii) the fight against illegal content and harmful conduct online; (iii) promoting a safer online environment; and (iv) establishing a knowledge base of all issues related to the achievement of a safer internet, such as the (evolving) ways children use online technologies, the associated risks and the possible harmful effects the use of online technologies can have on them, including technical, psychological and sociological issues. The new Safer Internet Plus Programme was adopted in December 2008.[314]

3–109 Recommendations on the protection of minors and human dignity—Another set of EU initiatives in the field of regulating illegal and harmful content are the complementary 1998[315] and 2006[316] Recommendations on protecting minors and human dignity.

3–110 ***1998 Recommendation***—The 1998 Recommendation is considered to be the most comprehensive legal instrument establishing a framework for the protection of minors in new media services, and was the first legal instrument at the EU level concerning the content of all electronic audiovisual and information services, regardless of the means of conveyance.[317] The 1998 Recommendation is based on the principle that the development of a competitive audiovisual and information services industry depends on the creation of a climate of public confidence, and hence on the protection of certain important general interests, such as the protection of minors and human dignity. The 1998 Recommendation emphasises the potential for self-regulation, and creates guidelines for the development of national self-regulatory frameworks to protect minors, as a supplement to the regulatory framework. Key building blocks set out in the 1998 Recommendation are codes of conduct, parental control tools, hotlines, awareness actions, multi-stakeholder involvement and cross-border cooperation. The 1998 Recommendation is addressed to the Member States. They are encouraged to: (i) promote the establishment of voluntary national frameworks, according to the guidelines in the Annex; (ii) encourage broadcasters to undertake research on new means to protect minors; (iii) set up hotlines and cooperation between complaints-handling structures to fight illegal content; and (iv) promote awareness on the responsible use of information services and identification of and access to quality content. Nevertheless, the 1998 Recommendation also indicated that the industries and parties concerned should: (i) set up structures to improve coordination at the EU and international levels; (ii) draw up codes of

[312] Proposal for a Decision of the European Parliament and of the Council establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, COM (2008) 106 final, 3.

[313] *ibid.*

[314] Decision 1351/2008 of December 16, 2008 establishing a multiannual Community Programme on protecting children using the Internet and other communication technologies, O.J. 2008 L348/118.

[315] Recommendation 98/560 of September 24, 1998, on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, O.J. 1998 L270/48.

[316] Recommendation 2006/952 of December 20, 2006, on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, O.J. 2007 L378/72.

[317] Recommendation 98/560, para.3–109, n.315, recital 5.

conduct; (iii) develop and experiment with new means of protecting minors and informing viewers; (iv) develop positive measures for the benefit of minors; and (v) collaborate in regular follow-ups and evaluations of initiatives in the framework of the 1998 Recommendation. Additionally, the Commission is responsible for facilitating the networking between the different actors, encouraging cooperation (and the sharing of experiences and good practices) between Member States and between self-regulatory and complaints-handling structures, promoting international cooperation and developing an evaluation methodology. The Annex to the Recommendation contains indicative guidelines for the implementation, at national level, of a self-regulation framework for the protection of minors and human dignity in on-line audiovisual and information services. These guidelines are built around four key elements: (i) consultation with and the representativeness of the parties concerned; (ii) codes of conduct; (iii) national bodies facilitating cooperation at the EU level; and (iv) national evaluation of self-regulatory frameworks.

3–111 ***2006 Recommendation***—In 2003, it was considered that the 1998 Recommendation should be updated. As a result, in December 2006, the Recommendation on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry was adopted.[318] The 2006 Recommendation is based on four main pillars: (i) awareness, education, media literacy and information campaigns, mainly aimed at the Member States; (ii) the development and use of filtering systems linked with content labelling (primarily aimed at industry and other parties involved); (iii) codes of conduct by professionals and regulatory authorities linked with quality labelling, aimed at industry and Member States; and (iv) a number of separate proposals which should be initiated by the Commission, *e.g.* a free telephone number informing users about complaint mechanisms and the effectiveness of filtering software, and a second level domain name ".kid.eu".

3–112 **Framework Decision on child pornography**—In order to address the issue of child pornography on the internet, a Framework Decision on combating the sexual exploitation of children and child pornography was adopted in 2003.[319] This Framework Decision requires Member States to ensure that the following intentional acts involving child pornography are punishable by imprisonment of up to 10 years when these acts, in part or in whole, are committed through the use of a computer: (i) production, (ii) distribution, dissemination or transmission, (iii) supplying or making available and (iv) acquisition or possession, of child pornography. This covers not only sexually explicit visual representations of children (*i.e.* persons under 18 years of age), but also images of persons whose age is unknown but who appear to be a child (although there is an exemption from liability where it can be established that the person is not a child), and images that are altered or even entirely generated by a computer in order to appear to be images of children. In its 2007 report on the Framework Decision, the European Commission emphasised the need to revise the Framework Decision, in particular to deal with offences related to developments in electronic communications technologies.[320] In March 2010, the Commission adopted a proposal for a Directive on combating the sexual abuse, sexual exploitation of children and child pornography,

[318] Recommendation 2006/952, see para.3–109, n.316, above.

[319] Framework Decision 2004/68/JHA of the Council of December 22, 2003 on combating the sexual exploitation of children and child pornography, O.J. 2004 L13/44.

[320] Report from the Commission based on Article 12 of Council Framework Decision 2004/68/JHA of December 22, 2003 on combating the sexual exploitation of children and child pornography, COM (2007) 716 final, (November 16, 2007).

repealing Framework Decision 2004/68/JHA.[321] The proposal focuses on the criminalisation on new forms of sexual abuse and exploitation facilitated by the use of the internet. This includes knowingly obtaining access to child pornography, to cover cases where viewing child pornography from websites without downloading or storing the images does not amount to "possession of" or "procuring" child pornography, and "grooming" of children for sexual purposes.

G. Electronic commerce

3–113 The use of the internet for commercial activities raises a number of challenging legal issues. These include questions relating to contract law (*e.g.* contract formation, determination of payment timing and location and the application of the rules of evidence to internet transactions),[322] liability, conflict of laws[323] and taxation.[324] It is beyond the scope of this work to provide a comprehensive and exhaustive review of these issues and reference should be made to specialised publications on this subject.[325] This section will focus on the specific regulatory initiatives at the EU level to address the issues resulting from the commercial use of the internet, in the fields of electronic commerce, distance selling and marketing, and electronic money.

[321] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography repealing Framework Decision 2004/68/JHA, COM (2010) 94 final (March 29, 2010). In March 2009 the Commission had already published a Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2009) 135 final (March 25, 2009), but this proposal was withdrawn due to the entry into force of the Lisbon Treaty.

[322] For a comparative review of the treatment of these issues in the national laws of the US and a number of European countries, see Spindler and Börner, *E-Commerce Law in Europe and the USA* (Springer, 2002).

[323] See, *e.g.* Gillies, "A Review of the New Jurisdiction Rules for Electronic Consumer Contracts within the European Union" (2001) 1 *Journal of Information Law & Technology*; Höning, "The European Directive on e-Commerce (2000/31/EC) and its Consequences on the Conflict of Laws", (2005) 5 *Global Jurist Topics* 2; Van Overstraeten, "Surfing through Governing Laws on the Internet" (1998) *International Business Law Journal*; Dutson, "The Internet, the Conflict of Laws, Litigation and Intellectual Property: the Implications of the International Scope of the Internet on Intellectual Property Infringements" (1997) *Journal of Business Law* 495; and Burnstein, "Conflict on the Net: Choice of law in Transnational Cyberspace" (1996) 29 *Vanderbilt Journal of Transnational Law* 75.

[324] For a review of the tax issues raised by the use of the internet, see Le Gall, "Trading on Internet, Tax Aspects" (1998) *International Business Law Journal* 357; Parrilli, "The Server as Permanent Establishment in International Grids", in Altmann *et al.* (eds.), *Grid Economics and Business Models, Lecture Notes in Computer Science*, No.5206 (2008), 89–102; Parrilli, "E-Commerce and Transfer Pricing. Some Selected Issues" (2008) 2 (2) *Masaryk University Journal of Law and Technology* 83–97. For a comparative study of the taxation of e-commerce in the EU, the United States, Japan and a number of other countries, see Doernberg, Hinnekins, Hellerstein and Li, *Electronic Commerce and Multijurisdictional Taxation* (2001).

[325] See generally, Gringras, para.3–005, n.9; Chissick and Kelman, para.3–005, n.9; Hance, para.3–001, n.1; Reed and Angel (eds.), *Computer Law—The Law and Regulation of Information Technology* (6th edition, 2007); Büllesbach, Poullet and Prins (eds.), para.3–039, n.80; Todd, *E-Commerce Law* (2005); and Lodder and Kaspersen (eds.), *eDirectives: Guide to European Union Law on E-Commerce—Commentary on the Directive on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection* (2002).

1. E-Commerce Directive

3–114 Country of origin principle—The European Parliament and the Council adopted the E-Commerce Directive on June 8, 2000.[326] The aim of this Directive was to remove a number of obstacles that had been encountered by undertakings in providing online services, in particular as a result of the need for providers of online services to comply with divergent national regulations. Uncertainty as to which Member State's rules applied to e-commerce activities was also a difficulty, in particular as regards Member States' ability to regulate the provision of services supplied from other Member States. These obstacles were preventing the development of information society services in the common market and the creation of an internal market in these services. The E-Commerce Directive is an internal market initiative based on the principle of free movement enshrined in EU law, and therefore adopts the "country of origin" principle, which allows undertakings providing information society services which are authorised in one Member State to provide services throughout the common market. An information society service provider will, under the "country of origin" principle, be subject only to the laws of the Member State in which it is established.[327] Therefore, Member States may not restrict, within the fields coordinated by the E-Commerce Directive, the provision of information society services by undertakings established in other Member States, except in very limited circumstances.[328]

3–115 Scope—The objective of the E-Commerce Directive is to ensure the free movement of information society services in the internal market, by harmonising national laws on information society services.[329] It does this by establishing specific harmonised rules only in a limited number of areas necessary to ensure the functioning of the internal market. These include national laws on the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlement procedures, court actions and cooperation between Member States.[330] However, it does not establish additional rules on private international law and the jurisdiction of the courts.[331] The E-Commerce Directive does not affect the application of existing laws in the fields of taxation, data protection, competition law, the activities of notaries and lawyers, and gambling activities,[332] nor does it affect EU or national laws that promote cultural and linguistic diversity and the defence of pluralism.[333] It complements EU law, including on the protection of public health and the protection of consumers, all of which continues to be applicable to electronic commerce.[334]

3–116 Exclusions from the scope of the E-Commerce Directive—A number of fields are explicitly excluded from the scope of the "country of origin" principle, so that Member States may continue to apply national legislation to information society service providers established in other

[326] E-Commerce Directive, para.3–022, n.30.
[327] *ibid.*, Art.3(2). The "coordinated fields" are requirements of national law applicable to providers of information society services and to information society services, whether of a general or specific nature, concerning the taking up of the activity of an information society service (*e.g.* qualifications, authorisations and notifications) and the pursuit of an information society service (*e.g.* quality or content of the service, advertising, contracts and the liability of the service provider): *ibid.*, Art.2(h).
[328] *ibid.*, Art.3(2).
[329] *ibid.*, Art.1(1) and (2).
[330] *ibid.*, Art.1(2).
[331] *ibid.*, Art.1(4).
[332] *ibid.*, Art.1(5).
[333] *ibid.*, Art.1(6).
[334] *ibid.*, Art.1(3).

Member States. The excluded fields are: copyright and neighbouring rights; electronic money; insurance; the freedom of parties to choose the law applicable to the contract; consumer contracts; and certain real estate contracts and unsolicited commercial communications by email.[335] This means that, in these fields, providers of information society services will continue to be subject to regulation by any Member State in which they do business, as well as by the Member State of establishment, unless other EU law is applicable. Furthermore, by way of derogation from Article 3(2), Member States may, under certain conditions, restrict the freedom to provide information society services for reasons of public policy, public health, public security and consumer/investor protection, provided there is a serious and grave risk of prejudice to those objectives and that the restrictions are proportionate to the objective to be achieved.[336] However, Member States may only act if the Member State of establishment has been requested to take appropriate measures and has either taken no measures, or inadequate measures, and the Commission and the Member State of establishment have been informed that such measures will be taken,[337] save in situations of urgency.[338] The Commission must then examine whether such measures are compatible with EU law; if not, it must ask the Member State in question to refrain from taking such measures.[339]

3–117 Place of establishment of information society service providers—A provider of information society services is deemed to have its establishment in the Member State where it pursues an economic activity using a fixed establishment for an indeterminate duration.[340] Accordingly, the place of establishment of an undertaking providing services via an internet website is not necessarily the country in which the server and technology supporting its website are located,[341] nor the countries in which its website are accessible. Likewise, the place of establishment does not depend on the fact that a service provider established in one Member State offers services targeted at the territory of another Member State. In the event that a supplier is established in two or more Member States, the supplier will, for the purposes of the E-Commerce Directive, be considered to be established in the Member State where it has the centre of its activities, in accordance with the Court's case law.[342]

3–118 No prior authorisation—To ensure that establishing an information society service provider is not an activity subject to bureaucratic burdens, Member States may not make the provision of such services subject to prior authorisation or any procedure having equivalent effect.[343] However, Member States may require information society service providers to comply with authorisation schemes not specifically targeted at information society services. For example, if EU or national legislation requires professional qualifications or authorisation by a professional body in order to carry on a particular professional activity, this requirement will apply in full to any undertaking wishing to carry on such professional or business activities by means of the internet. In addition, information society services that constitute electronic communications

[335] *ibid.*, Art.3(3) and Annex.
[336] *ibid.*, Art.3(4).
[337] *ibid.*
[338] *ibid.*, Art.3(5).
[339] *ibid.*, Art.3(6).
[340] *ibid.*, Art.2(c). See also Case C-221/89, *R. v Secretary of State for Transport, ex p. Factortame Ltd* [1991] E.C.R. I-3905.
[341] E-Commerce Directive, para.3–022, n.30, Art.2(c), last sentence, and recital 19.
[342] Case C–56/96, *VT4 Ltd v Vlaamse Gemeenschap* [1997] E.C.R. I-3143. See also E-Commerce Directive, para.3–022, n.30, recital 19.
[343] E-Commerce Directive, para.3–022, n.30, Art.4(1).

services (*e.g.* internet access services) remain subject to the general authorisation requirements or individual rights of use under the Electronic Communications Regulatory Framework.[344]

3–119 General information to be provided by information society service providers—Member States must ensure that providers of information society service provide certain information to customers and to national authorities. Information society service providers must furnish at least the following information to the recipients of their services and the competent authorities, in an easily, directly and permanently accessible form: their name, and, where relevant, trade register and registration number (if any); geographical address; contact details (including an email address); relevant supervisory or professional authorisations (if any); and VAT number.[345] In addition, where information society services refer to prices, these must indicate whether they are inclusive of taxes and delivery costs.[346] This obligation supplements information requirements laid down in the Distance Contracts Directive.[347] Thus, even if no contract is concluded, a provider of information society services must make available this information, for example, on its website. In its First Report on the Application of the E-Commerce Directive (which dates from 2003), the Commission noted that these provisions had been transposed by almost all the Member States and the EFTA States, but there remained an awareness problem amongst internet operators.[348] The Report, however, also stated that information society service providers in general responded promptly and positively when failures to comply were pointed out to them. In addition to this general information obligation, providers must also furnish specific items of information concerning commercial communications and the conclusion of online contracts.[349]

3–120 Commercial Communications—The E-Commerce Directive establishes the principle that commercial communications must be clearly identifiable "as such", that is, as being commercial in nature.[350]

3–121 ***Concept of "commercial"***—The E-Commerce Directive does not give specific guidance on how to determine when a commercial communication is "identifiable as such". Common sense rules, as well as concepts and criteria used in media law,[351] can be applied to determine when the provision's requirements are satisfied, for example the use of colour schemes or formatting devices

[344] On the requirements of the Authorisation Directive, see para.1–153 *et seq.*, above.
[345] E-Commerce Directive, para.3–022, n.30, Art.5(1).
[346] *ibid.*, Art.5(2).
[347] Directive 97/7 of May 20, 1997 on the protection of consumers in respect of distance contracts, O.J. 1997 L144/19 ("Distance Contracts Directive"). See para.3–161 *et seq.*, below.
[348] European Commission, First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), November 21, 2003, COM(2003) 702 final, 9.
[349] See para.3–120 *et seq.*, below.
[350] E-Commerce Directive, para.3–022, n.30, Art.6(a). This obligation is in addition to any other information requirements imposed by EU law. A commercial communication is any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person, pursuing a commercial, industrial or craft activity or exercising a liberal profession. The following do not in themselves constitute commercial communications: (i) information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an email address; and (ii) communications relating to the goods, services or images of the company, organisation or person compiled in an independent manner, in particular without financial consideration; *ibid.*, Art.2(g).
[351] Under EU broadcasting law, the separation between commercial communication and editorial content has always been one of the leading principles for television advertising and teleshopping; see paras.2–064 and 2–107.

to separate out the commercial part of the communication.[352] Both the content and context of the communication are relevant in this regard: a message can be qualified as commercial when it carries the words "promotion" or "advertisement" in its title or body, but it need not necessarily include such terms when the content itself clearly promotes goods or services. There will often be borderline cases, when it is not clear if a communication is purely "commercial" in nature; for instance, a newsletter that purports to give an objective evaluation of products, but in fact contains editorial content promoting a particular one. In the light of the purpose of the identification obligation (protecting consumers and providing transparency to individuals, so that they are able to use information society services in an informed way), such a newsletter is likely to be considered as a commercial communication.[353]

3–122 ***Identification of the sender***—In addition, the natural or legal person on whose behalf the commercial communication is made must be clearly "identifiable".[354] The use of the term "identifiable", rather than "identified", shows that it is not necessary in every instance to list in detail the major contact details. It can be sufficient if the party on whose behalf the advertisement is made can be identified by clicking on a hyperlink, for instance, in an online banner advertisement, or in SMS advertising on mobile phones with limited screen space.[355] The interaction with other EU law instruments could, however, lead to more stringent obligations. For example, the Karlsruhe Regional Court found that the operator of an online lottery did not satisfy its obligations to provide information under the national law implementing the E-Commerce and Distance Contracts Directives by making its address available solely via a hyperlink; instead, it should have indicated its address clearly on its online order form. In other words, a hyperlink should be used only to the extent that it is not practicable to list all the required information directly.[356] Likewise, promotional competitions, games or offers (such as discounts, premiums and gifts), where authorised by the Member State in which the service provider is established, must be clearly identifiable as such, and the conditions for participation or qualification must be easily accessible and be presented accurately and unequivocally.[357]

3–123 Unsolicited Communications—The E-Commerce Directive also sets out an identification obligation with regard to unsolicited commercial communications transmitted by email (also referred to as "spamming"). Unsolicited communications should be clearly identifiable, so that the recipient can instantly identify such emails as being a commercial communication without having to open them.[358] Member States must also take measures to ensure that service providers making unsolicited commercial communications by email consult regularly and respect the opt-out registers in which natural persons not wishing to receive such commercial communications can register themselves.[359] It is important to note that, firstly, these provisions are without prejudice to the rules concerning unsolicited marketing in EU data protection legislation (currently laid down in Article

[352] Büllesbach, Poullet and Prins (eds.), para.3–039, n.80, 236.
[353] *ibid.*, 235.
[354] E-Commerce Directive, para.3–022, n.30, Art.6(b).
[355] Büllesbach, Poullet and Prins (eds.), para.3–039, n.80, 236.
[356] *ibid.*, 236.
[357] E-Commerce Directive, para.3–022, n.30, Arts.6(c) and (d).
[358] *ibid.*, Art.7(1).
[359] *ibid.*, Art.7(2).

13 of the E-Privacy Directive)[360] and in the Distance Contracts Directive.[361] Secondly, the question whether unsolicited communication via email is permitted or not, is excluded from the application of the "country of origin" principle in the E-Commerce Directive;[362] compliance is to be determined under the law of the country of the recipient of an unsolicited commercial email.

3–124 Regulated professions—The E-Commerce Directive contains specific rules on e-commerce activities conducted by members of regulated professions (such as accountants, doctors and lawyers).[363] Commercial communications that are part of an information society service provided by a member of a regulated profession must comply with the relevant professional rules, including those on the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and the members of the profession.[364] Member States and Commission must encourage professional associations and bodies to establish codes of conduct to govern the information society service activities of their members.[365] The Commission may also draw up proposals for EU initiatives to ensure the cross-border provision of professional services via the internet, and must take account of such codes of conduct.[366]

3–125 Electronic contracts—The E-Commerce Directive aims to promote the development of e-commerce. Therefore, it obliges the Member States to ensure that their legal systems do not hinder the conclusion of online contracts by imposing or requiring formal requirements that electronic means cannot fulfil. Hence, Member States must ensure that their legal systems allow contracts to be concluded electronically. They must also ensure that the legal requirements applicable to contracts neither prevent the effective use of electronic contracts nor result in such contracts being deprived of legal effect and validity, on account of having been made electronically.[367] The E-Commerce Directive does not state the method that the Member States must follow to achieve equivalence between traditional and electronic contracts: they can either suppress such formal requirements, or they can refine them or interpret them in such a way as to allow electronic contracts to comply with those requirements.[368]

3–126 ***Derogation for certain categories of contracts***—Member States may declare that electronic contracts falling into the following categories can be excluded from the obligation to permit contracts to be concluded electronically: (i) contracts creating or transferring rights in real property

[360] Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. 2002 L201/37, as amended by the Citizen's Rights Directive, para.3–023, n.38, discussed in detail in Ch.1; see para.1–361, *et seq.*, above.

[361] Directive 97/7 of May 20, 1997 on the protection of consumers in respect of distance contracts, O.J. 1997 L144/19, as last amended by Directive 2005/29 of May 11, 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Directives 84/450, 97/7, 98/27 and 2002/65 and Regulation 2006/2004 (Unfair Commercial Practices Directive), O.J. 2005 L149/22.

[362] *ibid.*, Art. 3(3) and Annex.

[363] The term "regulated profession" is that provided for under EU law in either the Diplomas Directive (Council Directive 89/48 of December 21, 1988 on a general system for the recognition of higher-education diplomas awarded on completion of professional education and training of at least three-years' duration, O.J. 1989 L19/16, Art.1(d)), or in the Professional Education and Training Directive (Council Directive 92/51 of June 18, 1992 on a second general system for the recognition of professional education and training to supplement Directive 89/48/EEC, O.J. 1992 L209/25, corrigendum O.J. 1995 L17/20 and O.J. 1995 L30/40), Art.1(f): see E-Commerce Directive, para.3–022, n.30, Art.2(g).

[364] *ibid.*, Art.8(1).

[365] *ibid.*, Art.8(2).

[366] *ibid.*, Art.8(3).

[367] *ibid.*, Art.9(1).

[368] *ibid.*, recitals 34–35.

(other than rental rights); (ii) contracts that by law require the involvement of courts, public authorities or professionals exercising public authority (such as notaries); (iii) contracts of suretyship guaranteed by collateral securities furnished by private individuals; and (iv) contracts governed by family law and the laws of succession.[369] Member States must provide an explanation to the Commission for any derogation that they make in respect of contracts falling within these categories.[370]

3–127 ***Amendment of national law to permit electronic contracts***—The E-Commerce Directive accordingly places a positive obligation on Member States to identify and amend any national law that might prevent, limit or deter the use of electronic contracts. Examples of legal requirements which the Member States must examine and, where appropriate, amend are: (i) requirements as to the medium used for the contract, such as requirements that contracts be "on paper", "written" or "signed in writing"; (ii) that there be an original copy or that there be a certain number of originals; (iii) requirements as to human presence, for example, that contracts be negotiated or concluded by natural persons or in the physical presence of both parties; and (iv) requirements as to the involvement of third parties, for example, that the contract be concluded in the presence of witnesses.

3–128 Formation of contracts—Another information and transparency obligation is imposed in the context of the contractual process. Providers of information society services must explain clearly, comprehensively and unambiguously, and prior to the conclusion of the contract, the manner of the formation of a contract by electronic means.[371] In particular, the information to be provided to the recipient of the services must include: (i) the different technical steps to follow to conclude the contract, although contracting parties who are not consumers can agree otherwise; (ii) whether or not the concluded contract will be filed by the service provider and whether it will be accessible; (iii) the technical means for correcting input errors prior to the conclusion of the contracts; and (iv) the language(s) offered for the conclusion of the contract.[372] The service provider must also provide details of any relevant codes of conduct to which he subscribes and how these can be consulted electronically.[373] These obligations do not apply to contracts concluded exclusively by an exchange of emails or by equivalent individual communication.[374]

3–129 Liability of intermediary service providers—The E-Commerce Directive exempts information society service providers from liability for unlawful acts in certain circumstances. These exemptions are called "safe harbour" provisions. They address the concern that if intermediaries were held liable for the content supplied by others, on the grounds of being the "publisher" or "distributor" of such content, then they would not enter the market, due to the excessive legal risks, or would provide services under such restrictive conditions that use would be discouraged and the rights of users, such as the right to privacy or free speech, would be undermined or threatened (the so-called "chilling effect"). Exemptions from liability are applicable only when the information society service provider's activities are limited to the technical process of opening and giving access to a communication network over which information made available by third parties is transmitted and temporarily stored (or cached), *i.e.* for technical, automatic and passive activities.[375] They do not affect the ability of Member States' courts or administrative authorities to

[369] *ibid.*, Art.9(2).

[370] *ibid.*, Art.9(3).

[371] *ibid.*, Art.10(1).

[372] *ibid.*

[373] *ibid.*, Art.10(2).

[374] *ibid.*, Art.10(4).

[375] *ibid.*, recital 42.

require service providers to terminate or prevent infringements.[376] The "safe harbour" provisions cover three situations: where a service provider acts as a "mere conduit", performs caching activities, or provides hosting activities.

3–130 ***Mere conduits***—Information society service providers act as a "mere conduit" where they play a passive role in either transmitting in a communication network information provided by third parties, or in providing access to such network, provided that the information society service provider: (i) does not initiate the transmission; (ii) does not select the receiver of the transmission; and (iii) does not select or modify the information contained in the transmission.[377] The acts of transmission and providing access include the automatic, immediate and transient storage of the information transmitted, provided that this is done solely for the purpose of carrying out the transmission and the information is not stored any longer than reasonably necessary for the transmission.[378] Limitations on the liability of service providers cover liability, both civil and criminal, for all types of unlawful activities initiated by third parties online, including copyright infringement, unfair competition practices, misleading advertising and defamation.

3–131 ***Caching agents***—The E-Commerce Directive also exempts information society service providers from liability for unlawful acts, subject to certain conditions, when they act as "caching" agents for their customers.[379]

3–132 *Concept of "caching"*—Caching is the activity of the automatic, intermediate and temporary storage of information, for the purpose of making the transmission of information more efficient, by enhancing the performance and the speed of digital networks. Normally, this activity is not offered as a separate information society service,[380] but forms an integral part of transmission in digital networks.

3–133 *Conditions for caching exemption to apply*—Article 13 of the E-Commerce Directive lists five conditions that must be satisfied in order for the exemption of liability to apply. The provider (i) must not have modified the information; (ii) must have complied with the conditions on access to the information (for example, if a service has to be paid for, the cached page may not be accessible free of charge, or if a page contains banners, the revenues for that banner should flow to the provider that is entitled to receive them and not to the provider caching the page); (iii) must update the information regularly, according to the standards and rules widely recognised and used by the industry (this is, for instance, important to avoid citizens ordering goods and services online at prices which are outdated because the provider did not update the cached pages); (iv) must not have interfered with applications ("the lawful use of technology") that measure the use of information, such as statistical programs that keep track of the number of visitors for a certain web page; such that the provider caching the page must ensure that the web page does not get less hits as a result of the caching; and (v) must have acted expeditiously to remove or to disable access to the information as soon as he obtained actual knowledge of the fact that the information had been removed at the initial source, that access to it had been disabled or that a court or an administrative authority had ordered such removal or disablement.

3–134 *Duty of care on the service provider*—The last condition implies a duty of care of the

[376] *ibid.*, Arts.12(3), 13(2) and 14(3).
[377] *ibid.*, Art.12(1).
[378] *ibid.*, Art.12(2).
[379] See further, Büllesbach, Poullet and Prins (eds.), para.3–039, n.80, 250–255.
[380] The Commission has noted that caching does not constitute, as such, a separate exploitation of the information transmitted: Commission Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, COM (1998) 586 final, 28, O.J. 1999 C30/4.

provider caching the information: it will only escape liability if it acted expeditiously upon obtaining knowledge about the removal of the information at the source, the blocking of access to it or about the making of such an order. This contrasts with the regime for providers that are mere conduits, under which the provider is exempted from liability even if it was aware of the illegal information or if it could have taken action. On the other hand, the duty of care under Article 13 is lighter than the one provided for in Article 14 for hosting providers.

3–135 ***Hosting agents***—An exemption from liability also applies under certain conditions for hosting agents. "Hosting" is the storage of content provided by recipients of the service and at their request.[381] It can, for instance, consist of the provision of server space for a company's or an individual's web site, or for a newsgroup. A hosting provider cannot be held liable for the information stored by it if the following conditions are satisfied: [382] (i) (in civil and criminal proceedings) it did not have actual knowledge that the information or activity was illegal (for example, it did not know that the recipient was storing child pornography or material that infringed copyright, or that in a newsgroup information was being exchanged about where to obtain illegal material), and moreover, as regards claims for damages (*i.e.* in civil proceedings), it was not aware of facts or circumstances from which the illegal activity or information was apparent; and (ii) upon obtaining such knowledge or awareness, it has acted expeditiously to remove the information or to disable access to it. The last condition implies a duty of care of the provider. It has to take immediate action if it obtains knowledge or awareness of the illegality of information or an activity. This condition could lead to a "catch 22" situation for the provider, in that it should remove information promptly after having been alerted about its alleged illegal character (so as to benefit of the liability exemption), but be reluctant to remove the information (for fear of being held liable by the recipient of the service for wrongfully removing the material).[383] The E-Commerce Directive itself does not provide more clarity about the exact timing of intervention by the ISP, but leaves this matter to the Member States for (self-)regulation at the national level.[384]

3–136 Other obligations imposed on Member States—Member States are prohibited from imposing general obligations on information society service providers to screen or to actively monitor third party content while providing transmission, network access, caching and hosting activities, or to actively seek facts or circumstances indicating illegal activity.[385] However, Member States may oblige service providers to inform the public authorities of illegal activities undertaken or information provided by recipients of their service or to identify recipients of their service with whom they have storage agreements.[386] This does not affect orders made in accordance with national law to monitor specific activity, nor does it prevent Member States from imposing duties

[381] This is not limited to automatic and temporal activities such as the storage referred to in Articles 12 and 13 dealing with mere conduit and caching.
[382] Unless the recipient of the service has acted under the authority or the control of the provider: E-Commerce Directive, para.3–022, n.30, Art.14(2).
[383] Lodder and Kaspersen, para.3–113, n.325.
[384] Unlike the US Digital Copyright Millennium Act, the E-Commerce Directive does not contain "Notice and Takedown" procedures. Member States are free to develop their own specific requirements that must be fulfilled for the expeditious removal or disabling of information to take place. Nevertheless, the intention is that industry should develop voluntary codes of conduct: E-Commerce Directive, para.3–022, n.30, Art.16. See also McEvedy, "The DMCA and the E-Commerce Directive" (2002) 24(2) E.I.P.R. 65; and Valcke, "E-Commerce Directive", in Castendyk, Dommering and Scheuer (eds.), *European Media Law* (2008).
[385] E-Commerce Directive, para.3–022, n.30, Arts.15(1) and 16.
[386] *ibid.*, Art.15(2).

of care on service providers to detect and prevent certain types of illegal activities.[387] Member States and the Commission shall also encourage the development of codes of conduct designed to contribute to the proper implementation of the terms of the E-Commerce Directive.[388] Member States must also not discourage out-of-court settlements of disputes between service providers and recipients of their services, in particular for consumer disputes.[389] They must also ensure that court actions are available under national law to allow for the quick adoption of interim measures to terminate alleged infringements of the national legislation implementing the provisions of the E-Commerce Directive.[390] Member States must also determine appropriate sanctions for infringements of national law implementing the E-Commerce Directive that are effective, appropriate and dissuasive.[391]

3–137 Implementation and review—Member States were required to have implemented the E-Commerce Directive by January 17, 2002. The Commission is required to submit biennial reports on the application of the E-Commerce Directive and propose any changes needed to adapt it to legal, technical and economic developments in the field of information society services, in particular with respect to the prevention of crime, the protection of children and consumers and the proper functioning of the internal market.[392] The Commission shall thereby, in particular, analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, "notice and take-down" procedures and the liability of information society service providers following the taking down of content, as well as the need for additional conditions for the exemption from liability in the light of technical developments.[393] So far, the Commission only submitted one report, in 2003, to the European Parliament, the Council and the Economic and Social Committee. In this First Report on the E-Commerce Directive, the Commission noted that some Member States (including Spain, Portugal and Austria) had extended the "safe harbour" provisions to include also providers of hyperlinks and search engines, whilst in other Member States, the liability of linking and searching activities had been dealt with in case law.[394] As these national approaches did not appear to give rise to any internal market concerns, the Commission saw no reason to adapt the E-Commerce Directive. The E-Commerce Directive does not apply to information society services supplied by service providers established in third countries. However, in view of the global dimension of electronic commerce, the EU's rules should be consistent with international rules. Therefore, further changes to the E-Commerce Directive may be required to take account of international developments within international organisations such as the WTO, OECD and UNCITRAL on legal issues.[395]

3–138 Consumer e-commerce contracts relating to the harmonisation of national law—The E-Commerce Directive only concerns consumer contracts in so far as it enhances the level of consumer protection already provided for by other instruments; it may not diminish such protection.[396] The E-Commerce Directive complements, and coexists with, other EU legislation on the

[387] *ibid.*, recitals 47 and 48.
[388] *ibid.*, Art.16.
[389] *ibid.*, Art.17.
[390] *ibid.*, Art.18.
[391] *ibid.*, Art.20.
[392] *ibid.*, Art.21(1).
[393] *ibid.*, Art.21(2).
[394] See para.3–119, n.348, above.
[395] E-Commerce Directive, para.3–022, n.30, recital 58.
[396] *ibid.*, Arts.1(3), 3(3) and Annex.

jurisdiction of the courts in civil and commercial matters, the applicable law of contracts, distance selling, unfair contract terms in consumer contracts, indication of prices, sales of timeshares, injunctions to protect consumers' interests, liability for defective products and advertising of medical products.

3–139 ***Jurisdiction***—Jurisdiction in non-domestic matters is governed by the Brussels I Regulation.[397] The Regulation replaced and updated the Brussels Convention of 1968 on jurisdiction and enforcement of judgments in civil and commercial matters, to take account of new forms of commerce, including electronic commerce.[398] Under the Brussels I Regulation, the general principle of jurisdiction is that an individual or a business may be sued in the Member State where he or it is domiciled. The Brussels I Regulation contains a number of exceptions to this general rule, which are to be construed narrowly.[399]

3–140 ***Actions by consumers***—Consumers (*i.e.* persons acting outside their trade or profession) have the choice to bring proceedings related to contracts concluded by them either in the Member State in which they are domiciled or in the Member State in which the other party to the contract, whether a person or an undertaking, is domiciled[400] if the contract is: (i) for the sale of goods on instalment credit terms; (ii) for a loan repayable by instalments (or any other form of credit) made to finance the sale of goods; or (iii) made with a commercial or professional person or undertaking pursuing activities in the consumer's Member State or who otherwise "direct" their activities to the consumer's Member State.[401] The Brussels I Regulation thus adopts both "country of origin" and

[397] Council Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. 2001 L12/1 ("Brussels I Regulation"). The Brussels I Regulation entered into force on March 1, 2002 in all Member States (with the exception of Denmark, where it entered into force in July 2007). As the EU's most important trading partners were not parties to the Brussels Convention of 1968 (which preceded the Brussels I Regulation) and the 1980 Rome Convention on the law applicable to contractual obligations, O.J. 1991 C52/1, the EU, its Member States, and 46 other countries, including the United States, China and Japan, started negotiations in 1992 on a convention on jurisdiction and the recognition and enforcement of foreign court judgments. The original effort resulted in a Preliminary Draft Hague Convention, prepared in October 1999, which was further revised during a Diplomatic Conference in June 2001. The 2001 text left many problems unresolved. It became clear that some countries, particularly the United States, could not agree to the convention being considered, and efforts were redirected at a convention of more limited focus. On June 30, 2005, the Final Act of the Twentieth Session of the Hague Conference on Private International Law was signed on behalf of the Member States of the Conference. The Final Act includes a new multilateral treaty, the Convention on Choice of Court Agreements, available at: *http://www.hcch.net/index_en.php?act=conventions.text&cid=98*. Designed to promote international trade and investment through enhanced judicial cooperation, the Convention governs international business-to-business agreements that designate a single court, or the courts of a single country as the exclusive court(s) for resolution of disputes. It will not apply to agreements that include a consumer as a party, nor will it apply to purely domestic agreements in which the parties are resident in the same Contracting State and all other elements relevant to the dispute are connected only with that State.
[398] In 2007, the provisions of the parallel Lugano Convention of 1988, concluded between the EU Member States and the members of the European Free Trade Association (EFTA), *i.e.* Switzerland, Iceland and Norway, were aligned with the Brussels I Regulation. The revised Lugano Convention on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters was signed on October 30, 2007 in Lugano by the EU, Denmark and the three EFTA States, available at: *http://www.bj.admin.ch/etc/medialib/data/wirtschaft/ipr.Par.0022.File.tmp/20071030_entw_lugano_convention-e.pdf*. See also Opinion 1/03 *Lugano Convention* [2006] E.C.R. I-1145, in which the Court of Justice ruled that the EU has exclusive competence to conclude the new Lugano Convention. .
[399] Case 220/88, *Dumez France SA and Tracoba SARL v Hessische Landesbank* [1990] E.C.R. 49.
[400] Brussels I Regulation, para.3–139, n.397, Art.16(1).
[401] *ibid.*, Arts.15(1) and 16.

"country of destination" principles in relation to jurisdiction. Although the Brussels I Regulation does not specifically address the e-commerce context, this means that because a business-to-consumer (B2C) e-commerce website may be accessible to consumers located throughout the EU, undertakings doing business over the internet are, in principle, subject to the jurisdiction of all Member States in which their customers reside.[402]

3–141 ***Actions by service providers***—Service providers may bring a claim against a consumer only in the Member State in which the consumer is domiciled.[403] These rules may be departed from only by an agreement that: (i) is entered into after a dispute has arisen; (ii) allows the consumer to sue in courts other than those of the Member State where either the consumer or the service provider are domiciled; or (iii) confers jurisdiction on the Member State where both parties are domiciled or habitually resident.[404]

3–142 ***Tort, delict and quasi-delict***—Special rules apply in the event of matters relating to tort, delict or quasi-delict, which may be relevant to claims in respect of defective or dangerous goods or services supplied over the internet.

3–143 *Brussels I Regulation*—Under the Brussels I Regulation, courts can exercise jurisdiction over tortious acts in two manners: (i) the court of the place where the tortious act took place *(locus acti)* can exercise jurisdiction over all tort claims, regardless of whether the damage for which compensation is sought occurred in the state of that court or in another Member State; or (ii) the court of the place where the tortious act caused a damage *(locus damni)* can exercise jurisdiction over tort claims, seeking compensation only for the damage which occurred in the state of that court.[405] Courts in European countries have traditionally had difficulties in applying these principles to websites and potentially harmful content available thereon.

3–144 *Interpretation by national courts*—As websites are by their very nature available throughout the world, this, at least in theory, means that a potentially harmful act can cause damage, or is at least liable to cause damage, in all countries. In the past, some courts have therefore attempted to define under which conditions they are entitled to exercise jurisdiction over (the content of) a website. In particular, in France, courts have required a "sufficient" or "substantial" link to the territory (*e.g.* through the language used on the website) before exercising jurisdiction. In 2008, the Liège Court of Appeal in Belgium made a request for a preliminary ruling to the Court of Justice, asking for clarification with regard to the application of Article 5(3) of the Brussels I Regulation to cases of alleged harm caused by websites. The outcome of this case could have provided detailed guidance and certainty to owners and operators of websites as to the conditions under which a national court will be able to exercise jurisdiction over those websites, but was removed from the register on March 24, 2009.[406]

3–145 ***Other jurisdictional issues***—Recent judgments of the Court of Justice have identified

[402] See Motion, "The Brussels Regulation and E-Commerce—A Premature Solution to a Fictional Problem" (2001) 7(8) C.T.L.R. 209. The Commission's original proposal for a draft Regulation contained a recital that specifically stated that websites were deemed to be directed at all Member States in which they were accessible: European Commission, "Proposal for a Council Regulation (EC) on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters", COM(99) 348, O.J. 1999 C376/1.

[403] Brussels I Regulation, para.3–139, n.397, Art.16(2).

[404] *ibid.*, Art.17.

[405] *ibid.*, Art.5(3). Hence, either only one court (*i.e.* the court of the place of the tortious act) can exercise jurisdiction over multi-territorial damage claims, or various courts can each exercise jurisdiction over damage claims relating to their respective territories.

[406] Case C-584/08, *Real Madrid Football Club et al. v Sporting Exchange Ltd et al*, O.J. 2009 C141/36, removed from the register.

other problems in the application of the Brussels I Regulation.[407] This has, in particular, been the case when a party commences in bad faith an action in a jurisdiction which is not the competent one according to the Brussels I Regulation and argues that the case is not covered by the Regulation (*e.g.* arbitration clauses) or falls into the exceptions to the general rule. These actions launched in bad faith often use Article 28 of the Regulation on parallel actions (*lis pendens*) to delay the proceedings or to prevent the case from being brought in front of another court than the one they prefer. Article 28 provides that when the same case is brought before the courts of different Member States, the second court seized must suspend proceedings before it until the competence (or not) of the first court seized has been established.

3–146 ***Review of Brussels I Regulation***—The Commission announced that it will publish an implementation report on the Brussels I Regulation and launch a consultation on the review of the text in March 2009. This was expected to lead to the adoption by the Commission of a proposal to review the Regulation by the end of 2009.

3–147 **Applicable law of the contract**—The applicable law of a contract is governed by the Rome I Regulation.[408] The Rome I Regulation replaces the 1980 Rome Convention on the law applicable to contractual obligations.[409] It contains EU-wide rules to determine which country's law governs contracts when the contracting parties are not located in the same country. This instrument is particularly important for electronic commerce, as it applies to contracts that are concluded online or by using mobile phones. The Rome I Regulation applies to cross-border contractual civil and commercial matters, whether online and offline, whenever the competent court is the court of a Member State (except Denmark and the United Kingdom). It does not apply in a number of areas, including: (i) pre-contractual obligations; (ii) questions involving the status or legal capacity of individuals; (iii) corporate, family and administrative questions; and (iv) arbitration agreements and agreements on the choice of courts.[410]

3–148 ***General rule—freedom of choice***—The Rome I Regulation applies both to contracts that contain a choice of law clause and to those that do not. The general rule is that a contract is governed by the law chosen by the parties.[411] This freedom of choice principle also applies to consumer contracts, to the extent this does not deprive the consumer of the protection given by the rules, which cannot be derogated from by contract, of the law that would apply in the absence of

[407] For instance, Case C-159/02, *Gregory Paul Turner v Felix Fareed Ismail Grovit, Harada Ltd, Changepoint SA* [2004] E.C.R. I-3565; and Case C-185/07, *Allianz SpA (formerly Riunione Adriatica Di Sicurta SpA) v West Tankers Inc.*, [2009] E.C.R. I-663.

[408] Regulation 593/2008 of June 17, 2008 on the law applicable to contractual obligations (Rome I), *O.J. 2008 L 177/6* ("Rome I Regulation"). In 2007, a further regulation, the Rome II Regulation, was adopted, governing the applicable law in cases of non-contractual liability, such as product liability, unfair competition, or infringements of intellectual property rights: Regulation 864/2007 of the European Parliament and of the Council of July 11, 2007 on the law applicable to non-contractual obligations (Rome II), O.J. 2007 L199/40 ("Rome II Regulation"). Disputes relating to defamation and other infringements of privacy, whose inclusion was debated during the adoption process, are not covered. The general rule, laid down in Art.4, is that, in the absence of choice of the parties on the applicable law, the law of the country in which the damage is sustained applies, which will usually be the consumer's country of residence. The Rome II Regulation contains a number of specific rules for particular types of disputes, of which the most relevant ones for online activities are those on product liability (Art.5), acts of unfair competition and restriction of free competition (Art.6), and disputes over infringements of intellectual property rights (Art.8).

[409] Rome Convention, para.3–139, n.397.

[410] Rome I Regulation, para.3–147, n.408, Art.1.

[411] *ibid.*, Art.3.

choice (*i.e.* often the law of his home Member State).[412] However, even if a law is chosen by the parties, a court may have to apply some provisions of another country's law. This could be the case if all the other elements of the situation at the time of the choice are located in a country other than the one whose law has been chosen. In that case, the court will have to apply the mandatory rules of that other country, *i.e.* the rules that cannot be derogated from.[413] In addition, national "overriding mandatory provisions" or public policies could also exceptionally lead to the application of another law.[414]

3–149 ***Applicable law if no choice of law is made***—In the absence of the parties choosing the applicable law, the law of the jurisdiction of the habitual residence of the seller (or service provider) at the time of conclusion of the contract applies ("country of origin"), except for certain types of contracts, *i.e.* contracts concluded with consumers, carriage contracts, insurance contracts and individual employment contracts.[415] The habitual residence of companies, for the purpose of the Rome I Regulation, is the place of its central administration.[416] For consumer contracts, the applicable law (in the absence of choice) is the law of the Member State in which the consumer has his "habitual residence", provided either the trader carries out his activity in that Member State, or the trader directs, by any means, his activities to that Member State or to several countries, including that Member State and the contract falls within the scope of such activities.[417] These specific rules on consumer contracts do not apply to certain types of contracts, including those for the supply of services where the service is supplied in a country other than that of residence of the consumer.[418]

3–150 ***Exceptions***—A court may refuse to apply the law designated by the Rome I Regulation if its application would be manifestly incompatible with public policy ("ordre public").[419] It may also apply the overriding mandatory provisions (*i.e.* the provisions which are considered as crucial for the safeguard of a country's public interests) of the laws of either its own country, or the country where the contractual obligations must be performed, in so far as these provisions make the performance of the contract unlawful.[420] Therefore, in a number of situations, a service provider may be confronted with the application of the laws of countries other than the country of origin. The question arises as to whether this may contradict the country of origin principle underpinning the E-Commerce Directive.[421] Recital 40 of the Rome I Regulation specifies that the Regulation should not disrupt the application of internal market instruments *"insofar as they cannot be applied in conjunction with the law designated"* by the Regulation. Furthermore, and very specifically, it is stated that the application of provisions of the applicable law designated by the

[412] *ibid.*, Art.6(2).

[413] *ibid.*, Art.3(3). The same exception applies when all other elements relevant to the situation at the time of the choice are located in one or more Member States and if the chosen law is the law of a third country. In that case, the choice could not prevent the application of EU law provisions (as implemented in the Member State of the court) which cannot be derogated from: *ibid.*, Art.3(4).

[414] See para.3–150, below.

[415] *ibid.*, Art.4.

[416] *ibid.*, Art.19.

[417] *ibid.*, Art.6(1). If this is not the case, the general rules of Arts.3 and 4 will apply.

[418] *ibid.*, Art.6(4). These contracts will be governed by the general rules in Arts.3 and 4.

[419] *ibid.*, Art.21.

[420] *ibid.*, Art.9. Overriding mandatory provisions of domestic law are provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation, to such an extent that they are applicable to any situation falling within their scope, irrespective of the law otherwise applicable to the contract under the Rome I Regulation.

[421] See para.3–114, above.

rules of this Regulation should not restrict the free movement of goods and services as regulated by EU instruments, such as the E-Commerce Directive. In practice, conflicts between the applicable law designated by the Rome I Regulation and the country of origin principle of the E-Commerce Directive are unlikely: for contracts with consumers, the country of origin principle does not apply to contractual obligations with consumers, nor does it affect the freedom of the parties to choose the law applicable to their contract.[422] For contracts between businesses, conflicts are also likely to be rare as the Rome I Regulation will often lead to the application of the law of the seller or service provider (*i.e.* of the law of the country of origin). With regard to its relationship with other EU legislation, the Rome I Regulation specifically states that it does not apply whenever that legislation lays down conflict of law rules relating to contractual obligations.[423]

3–151 **Other matters on consumer contracts**—The EU has adopted a wide range of other legislation which, although not specifically directed at e-commerce, will have an effect upon it.

3–152 ***Subject-matter of other EU legislation***—EU legislation that may have an effect on e-commerce include measures dealing with the following topics: unfair terms in consumer contracts,[424] unfair commercial practices,[425] distance contracts with consumers,[426] information obligations and policies on quality,[427] misleading and comparative advertising,[428] consumer credit contracts,[429] package holidays,[430] the indication of prices,[431] product safety,[432] timeshare contracts,[433] injunctions to protect consumers' interests,[434] liability for defective products,[435] the sale of

[422] Electronic Commerce Directive, para.3–022, n.30, Art.3(3) and Annex.

[423] Rome I Regulation, para.3–147, n.408, Art.23. See, for instance, the provisions of the Distance Contracts Directive and of the Unfair Terms in Consumer Contracts Directive, which state that consumers cannot lose their protection by the contractual choice of the law of a third country, will apply irrespective of the rules of the Rome I Regulation.

[424] Council Directive 93/13 of April 5, 1993 on unfair terms in consumer contracts, O.J. 1993 L95/29 ("Unfair Consumer Contracts Directive").

[425] Unfair Commercial Practices Directive, para.3–123, n.361.

[426] Directive 97/7 of May 20, 1997 on the protection of consumers in respect of distance contracts, O.J. 1997 L144/19, as last amended by the Unfair Commercial Practices Directive, para.3–123, n.361 and Directive 2002/65 of September 23, 2002 concerning the distance marketing of financial services and amending Directives 90/619, 97/7 and 98/27, O.J. 2002 L271/16.

[427] Directive 2006/123 of December 12, 2006 on services in the internal market, O.J. 2006 L376/36 ("Services Directive").

[428] Directive 2006/114 of December 12, 2006 concerning misleading and comparative advertising (codified version), O.J. 2006 L376/21.

[429] Directive 87/102 of December 22, 1986 for the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit, O.J. 1987 L42/48, as last amended by Directive 98/7, O.J. 1998 L107/17.

[430] Directive 90/314 of June 13, 1990 on package travel, package holidays and package tours, O.J. 1990 L158/59.

[431] Directive 98/6 of February 16, 1998 on consumer protection in the indication of prices of products offered to consumers, O.J. 1998 L80/27.

[432] Directive 2001/95 of December 3, 2001 on general product safety, O.J. 2002 L11/4.

[433] Directive 2008/122 of January 14, 2009 on the protection of consumers in respect of certain aspects of timeshare, long-term holiday product, resale and exchange contracts, O.J. 2009 L33/10.

[434] Directive 98/27 of May 19, 1998 on injunctions for the protection of consumers' interests, O.J. 1978 L164/51, as last amended by the Services Directive, para.3–152, n.427 . It has been proposed that the Consumer Injunction Directive should be codified: COM(2003) 241 final (May 12, 2003) and COM(2006) 692 final (November 16, 2006).

[435] Directive 85/347 of July 25, 1985 on the approximation of the laws, regulations and administrative provisions concerning liability for defective products, O.J. 1985 L210/29, as amended by Directive 1999/34, O. J. 1999 L141/20.

consumer goods and associated guarantees,[436] the advertising of medical products,[437] and the advertising of tobacco products.[438] Despite the adoption of these various directives in the area of consumer protection,[439] this has not prevented a fragmentation of the "Consumer Acquis".

3–153 ***Risk of fragmentation of the internal market***—Because the generally-applicable directives enumerated above contain only minimum harmonisation clauses, Member States have made extensive use of the possibility to maintain or adopt stricter consumer protection rules. The result is a fragmented regulatory framework. The effects of this fragmentation on the internal market have led to reluctance by businesses to sell cross-border to consumers. Since, under the Rome I Regulation, consumers contracting with a foreign trader cannot be deprived of the protection stemming from the non-derogable rules of their home country, cross-border traders are faced with significant compliance costs. In addition, the level of consumer confidence in cross-border shopping still remains low.[440]

3–154 ***Proposal for a Consumer Rights Directive***—The European Commission has launched an initiative to simplify and update existing consumer protection directives, merging them into one directive. On October 8, 2008, it adopted the proposal for a Directive on Consumer Rights,[441] which aims to ensure a high level of consumer protection and to establish a real internal market in retailing, to make it easier and less costly for traders to make cross-border sales and to provide consumers with a larger choice and competitive prices. It will also modernise existing consumer rights, bringing them in line with technological change (*e.g.* m-commerce, online auctions).

3–155 **VAT and Electronically Supplied Services**—The imposition of VAT on e-commerce activities is governed by the VAT Directive 2006,[442] which repealed the E-Commerce Taxation Directive[443] and the Sixth VAT Directive.[444]

[436] Directive 99/44 of May 25, 1999 on certain aspects of the sale of consumer goods and associated guarantees, O.J. 1999 L171/12. This Directive will be repealed by the new Consumer Rights Directive, once it is adopted: see para.3–154, n.441, below.

[437] Directive 2001/83 of November 6, 2001 on the Community code relating to medicinal products for human use, O.J. 2001 L311/ 67, as last amended by Directive 2008/29 of March 11, 2008, O.J. 2008 L81/51 (repealing Directive 92/28 of March 31, 1992 on the advertising of medical products, O.J. 1992 L113/13).

[438] Directive 2003/33 of May 26, 2003 on the approximation of laws, regulations and administrative proceedings of the Member States relating to the advertising and sponsorship of tobacco products, O.J. 2003 L152/16.

[439] See also Regulation 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, O.J. 2004 L364/1, as last amended by the AVMS Directive, para.3–028, n.50.

[440] Eurobarometer results on e-commerce 2008, available at *http://ec.europa.eu/consumers/strategy/facts_eurobar_en.htm*. See also Commission Press Release, *Gap between domestic and cross-border e-commerce grows wider, says EU report*, IP/08/980 (June 20, 2008).

[441] Commission, "Proposal for a Directive of the European Parliament and of the Council on consumer rights", COM (2008) 614 final; available at *http://ec.europa.eu/consumers/rights/cons_acquis_en.htm* (proposed "Consumer Rights Directive").

[442] Directive 2006/112 of November 28, 2006 on the common system of value added tax, O.J. 2006 L347/1 ("VAT Directive 2006"). For a more in-depth analysis of the European VAT regime applicable to e-commerce services (including a discussion of Directive 2008/8, which will be in force from 2010–2015; see n.448, below), see Parrilli, "European VAT and Electronically Supplied Services" (2008), available at: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261822*.

[443] Directive 2002/38 of May 7, 2002 amending temporarily Directive 77/388 as regards the value added tax arrangements applicable to radio and television broadcasting services and certain electronically supplied services, O.J. 2002 L128/41. At the same time, the Council also adopted Regulation 792/2002 of May 7, 2002 amending temporarily Regulation (EC) 218/92 on administrative cooperation in the field of indirect taxation (VAT) as regards additional measures regarding e-commerce, O.J. 2002 L128/1.

[444] Directive 77/388 of May 17, 1977 on the harmonisation of the laws of the Member States relating to turnover taxes—Common system of value added tax: uniform basis of assessment, O.J. 1997 L145/1.

3–156 ***Position under the Sixth VAT Directive***—Under the Sixth VAT Directive, suppliers established in the EU were obliged to charge VAT when selling their products to customers located outside the EU, while third country suppliers were not required to charge VAT on sales within the EU. This system distorted competition and hampered the functioning of the internal market.

3–157 ***VAT Directive 2006***—The VAT Directive 2006, following the principles contained in the E-Commerce Taxation Directive, eliminated the distortions of competition in the supply of e-commerce services to consumers that resulted from the application of the Sixth VAT Directive. The VAT regime applicable to e-commerce between businesses remains unchanged, and the place of taxation is the customer's Member State whether or not the supplier is based in the EU. Furthermore, VAT is not levied on for the provision of e-commerce services by a supplier established in the EU to a customer (whether business or consumer) established outside the EU.

3–158 *Special scheme for supply of electronic services to consumers*—The central provision of the E-Commerce Taxation Directive (and of the VAT Directive 2006) is the establishment of a special scheme for the taxation of electronically supplied services provided to (non-taxable) consumers within the EU by service providers that are not established in the EU. The general principle for the taxation of such services is that they should be taxed at the rate applicable in the Member State in which the recipient of these services is located. Providers established in third countries are required to choose a particular Member State—the "Member State of identification"—from which it is to receive a VAT identification number.[445] They must then submit, on a quarterly basis, to the Member State of identification a VAT return that sets forth the identification number and, for each individual Member State of consumption where tax has become due, the total value, less VAT, of the electronic services supplied and the total amount of the corresponding tax.[446]

3–159 *Position until December 31, 2014*—Until the end of 2014, the provision of e-services by a supplier based in the EU to a consumer established in another Member State will be taxed in the supplier's country. Furthermore, the VAT Directive 2006 is intended to provide a coherent system for levying VAT on electronically supplied services, including: (i) website supply, web-hosting and distance maintenance of programs and equipment; (ii) supply and updating of software; (iii) supply of music, films and games, including games of chance and gambling games, and of political, cultural, artistic, sporting, scientific and entertainment broadcasts and events; and (iv) supply of distance teaching. However, the mere fact that a supplier of a service and a customer communicate by email does not necessarily mean that the service provided is an electronic service.[447]

3–160 *New scheme from 2015*—From the beginning of 2015, according to the provisions of Directive 2008/8,[448] this special scheme will be formally replaced by a special scheme for telecommunications, broadcasting or electronic services supplied by taxable persons not established within the EU (which will be the same as that described above) and another special regime will

[445] VAT Directive 2006, para.3–155, n.442, Art.362. Pursuant to Art.361, the service provider must provide the Member State of identification with the following information: name; postal address; electronic addresses (including websites); national tax number, if any; and a statement that the person is not registered for value added tax purposes within the EU.

[446] *ibid.*, Art.364.

[447] *ibid.*, Art.56(3).

[448] Directive 2008/8 of February 12, 2008 amending Directive 2006/112 as regards the place of supply of services, O.J. 2008 L44/11.

apply for telecommunications, broadcasting or electronic services supplied by taxable persons established within the EU but not in the Member State of consumption. The latter special scheme will be applicable to taxable persons who have established their business in the territory of the EU or have a fixed establishment there, but not within the territory of the Member State of consumption[449] and will imply that the place of taxation will be the Member State of identification at the rate of the customer's Member State.

2. Regulatory framework for distance selling and marketing

3–161 The EU has adopted three legislative measures on consumer protection that are particularly relevant to e-commerce: the Distance Contracts Directive,[450] the Financial Services Distance Marketing Directive,[451] and the Framework Decision on Combating Fraud and Counterfeiting.[452] The Commission has also issued a Communication on e-commerce and financial services,[453] in which it lays out its policy framework for completing the internal market in financial services.

3–162 The Distance Contracts Directive—Many consumer contracts are concluded without the consumer and the supplier ever coming into physical contact with one another, *i.e.* at a "distance". The harmonisation of national laws on distance selling was an important and necessary step in completing the internal market in goods and services, as different and/or divergent national rules affected competition and the cross-border provision of goods and services. It was also necessary to ensure a harmonised level of consumer protection throughout the EU. For the purposes of the Distance Contracts Directive, distance selling is defined as the conclusion of a contract regarding goods or services whereby the contact between the consumer and the supplier takes place by means of technology for communication at a distance.[454] The use of distance communication means that the two parties are not simultaneously physically present.[455] This form of selling goods and services covers a wide range of trade activities, including traditional forms such as telephone press advertising, mail-order catalogues and personal mailing, but also modern techniques of distance selling such as the internet, email or automated telephone calls and faxes.[456]

3–163 ***Information to be provided to the consumer***—The service supplier must provide certain information to the consumer prior to the conclusion of the contract. The information to be provided includes: the identity of the supplier; his address (in the case of payment in advance); the main characteristics of the goods or services; the price, including taxes and delivery costs; the arrangements for payment, delivery or performance; the existence of a right of withdrawal; the costs of using the means of communication at a distance (if other than at the basic rate); the

[449] Called "non-established taxable persons": see VAT Directive 2006, para.3–155, n.442, Art.358(1).
[450] Distance Contracts Directive, para.3–152, n.426. For a comprehensive review of the Distance Contracts Directive, see Chissick and Kelman, para.3-005, n.9.
[451] Directive 2002/65 of September 23, 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619 and Directives 97/7 and 98/27, O.J. 2002 L271/16.
[452] Council Framework Decision 2001/413 of May 28, 2001 on combating fraud and counterfeiting of non-cash means of payment, O.J. 2001 L149/1.
[453] Communication from the Commission, "E-commerce and Financial Services", available at: *http://europa.eu.int/comm/internal_market/en/finances/general/ecom.htm.*
[454] Distance Contracts Directive, para.3–152, n.426, Arts.2(1) and 2(4).
[455] *ibid.*
[456] *ibid.*, Annex I. Some of these forms of direct marketing are regulated under EU law: see paras.3–121 and 3–123, above.

period for which the offer or the price remains valid; and the minimum duration of the contract.[457] This information must be provided in a clear, comprehensive and appropriate way, respecting the principles of good faith in commercial transactions and the principles governing the protection of those who are unable under national law to give their consent, such as minors.[458]

3–164 ***Written confirmation of information***—The consumer must receive written confirmation (or confirmation in another durable medium) of the following information: the identity of the supplier; his address (in the case of payment in advance); the main characteristics of the goods or services; the price, including taxes and delivery costs; the arrangements for payment, delivery or performance; the existence of a right of withdrawal, after-sales services and guarantees; and the conditions for cancelling the contract, if it is of unspecified duration or for more than one year.[459] This information must be provided in good time during the performance of the contract or, at the latest, at the time of delivery. This provision does not apply to the performance of services that are supplied on only one occasion and are invoiced by the operator of the communication network (*e.g.* premium rate telephone services), although consumers must always be able to obtain the geographical address of the service provider, where complaints may be addressed.[460] In the case of telephone communications, the identity of the supplier and the commercial purpose of the call must be made explicitly clear at the beginning of the conversation.[461]

3–165 ***Right of withdrawal***—The consumer must be given a right to withdraw from the contract, which can be exercised for at least seven working days after conclusion of the contract, with a limited number of exceptions (*e.g.* where performance of a contract for services has begun with the consumer's agreement; contracts for personalised goods; the sale of audio or video recordings; computer software that has been unsealed by the consumer; and/or magazines and newspapers).[462] Withdrawal must be free of charge for the consumer, except in relation to any direct costs for returning goods already delivered. Any reimbursement of sums already paid by the consumer must be done within three days of withdrawal.[463]

3–166 ***Performance***—Any order must be executed by the supplier within 30 days from the day following that on which the consumer forwarded his order to the supplier.[464] Where the supplier fails to perform his obligations under the contract on the ground that the goods or services ordered are unavailable, the consumer must be informed of this situation and must be able to obtain a refund of any sums he has paid as soon as possible and in any case within 30 days.[465] The consumer may be provided with goods or services of equivalent quality and price, provided the consumer was properly informed of this possibility before or during the conclusion of the contract. If such alternative goods are not acceptable to the consumer, the supplier must bear the costs of returning them and the consumer must be informed of this.

3–167 ***Payment by card***—The Distance Contracts Directive originally provided that Member States had to ensure that in the case of fraudulent use of a payment card (*e.g.* a credit or debit card), the consumer was able to request cancellation of the order and reimbursement of the sums

[457] *ibid.*, Art.4.
[458] *ibid.*, Art.4(2).
[459] *ibid.*
[460] *ibid.*, Art.5(2).
[461] *ibid.*, Art.4(3).
[462] *ibid.*, Art.6(1) and (3).
[463] *ibid.*, Art.6(2).
[464] *ibid.*, Art.7(1).
[465] *ibid.*, Art.7(2).

paid.[466] This provision was criticised, as it was limited to payment by card and did not apply to new payment methods such as electronic money, and because it was not applicable in case of defective execution, non-execution or negligence by the issuer of the card.[467] This requirement was repealed by Directive 2007/64 on payment services in the internal market.[468]

3–168 ***Inertia selling***—The Unfair Commercial Practices Directive[469] prohibits the supply of goods or services to a consumer without the consumer having ordered these if such supply involves a demand for payment (so-called "inertia selling"). In the light of that provision, Member States shall take measures necessary to exempt the consumer from being obliged to pay for unsolicited goods or services, and the absence of a response by the consumer does not constitute consent and does not expose the consumer to liability to pay for the goods or services.[470]

3–169 ***Mandatory nature of the Distance Contracts Directive***—The consumer may not waive the rights conferred on him by national laws implementing the Distance Contracts Directive.[471] Simultaneously, Member States must ensure that consumers do not lose the benefits of consumer protection laws by virtue of the choice of the law of a third country as the law applicable to the contract, if the contract has a close connection with the territory of one or more Member States.[472]

3–170 ***Minimum level of guaranteed protection***—The Distance Contracts Directive ensures only the minimum level of harmonised consumer protection. Therefore, Member States may introduce or maintain more stringent provisions that are compatible with EU law , in order to ensure a higher level of consumer protection. In particular, the marketing of certain goods and services (*e.g.* medicinal products) may be prohibited within their territory.

3–171 ***Goods and services to which the Distance Contracts Directive is not applicable***—The Distance Contracts Directive does not apply to: contracts relating to financial services;[473] contracts concluded by means of automatic vending machines or automated commercial premises; contracts concluded with telecommunications operators through the use of public pay-phones; or contracts concluded for the construction and sale of immovable property or other property rights, except rentals.[474] Moreover, a number of obligations imposed by the Directive (*i.e.* prior information, written confirmation, right of withdrawal and performance) do not apply to contracts relating to the supply of foodstuffs, beverages or other goods intended for everyday consumption, accommodation, transport, catering and leisure.[475]

3–172 ***Implementation***—Member States were required to implement the Distance Contracts Directive by no later than June 4, 2000.

3–173 **Financial Services Distance Marketing Directive**—The provision of consumer financial services (such as investment services, insurance and reinsurance, banking and operations related to

[466] *ibid.*, Art.8.
[467] See Salaün, "Electronic payments and contracts negotiated through the internet" (1999) 5(2) C.T.L.R. 26.
[468] Directive 2007/64 of November 13, 2007 on payment services in the internal market amending Directives 97/7, 2002/65, 2005/60 and 2006/48 and repealing Directive 97/5, O.J. 2007 L319/1, Art. 89. This Directive will be repealed by the proposed Consumer Rights Directive, once it is adopted: see para.3–154, n.441, above.
[469] Directive 2005/29 of May 11, 2005 concerning unfair business-to-consumer commercial practices in the internal market, para.3–123, n.361.
[470] Distance Contracts Directive, para.3–152, n.426, Art.9.
[471] *ibid.*, Art.12.
[472] *ibid.*, Art.12(2).
[473] *ibid.*, Art.3(1)
[474] *ibid.*, Art.3(1).
[475] *ibid.*, Art.3.

dealings in futures and options) was exempted from the scope of the Distance Contracts Directive.[476] Following a broad consultation, the Commission concluded that there was a need to complete the internal market in financial services and to strengthen consumer protection in this field, in light of the growing importance of distance selling in the marketing of financial products and the specific issues raised by distance selling of financial services. Different and divergent national laws had also created serious obstacles to the cross-border provision of financial services by means of distance communications. For this reason, specific legislation was adopted in the financial services sector, although this sector was already regulated by a number of financial services directives, which overlap somewhat with the information obligations under the Distance Contracts Directive.[477] Following a number of Commission proposals,[478] on September 23, 2002 the Financial Services Distance Marketing Directive was adopted.[479] This Directive establishes a clear regulatory framework for the cross-border marketing of financial services, by approximating Member States' rules on the distance marketing of consumer financial services.[480] Suppliers of financial services can now offer their products throughout the EU, without the hindrance of having to comply with different national laws on the distance selling of consumer financial services.

3–174 ***Consumer protection provisions***—The Financial Services Distance Marketing Directive closely follows the approach of the Distance Contracts Directive. It applies the same definition of a distance contract, except that it applies only to financial services, rather than to goods and services generally.[481]

3–175 *Information to be provided to the consumer*—Certain information must be supplied to consumers before the conclusion of the contract.[482] This information includes: the name of the supplier, including its representative in the Member State of the consumer's residence and any professional intermediary; the financial service involved, including its characteristics, the total price or a method for calculating it, notice of any special risks related to the financial service and details of relevant taxes; the distance contract, including the existence, or otherwise, of a right of withdrawal, the minimum duration of the contract, right to early termination, and clauses on applicable law and jurisdiction; and redress, including out-of-court complaint and redress procedures, and the existence of guarantee funds and other compensation arrangements.[483] This information is more extensive than that required under the Distance Contracts Directive and reflects the specific nature of financial services products. As with the Distance Contracts Directive, this information must be provided in a clear, comprehensible and appropriate manner, having due regard to principles of good faith and the protection of those who may lack contractual capacity, such as children.[484]

3–176 *Application of other EU legislation*—If EU law imposes additional information requests on providers of financial services, these shall continue to apply, and, pending further

[476] *ibid.*
[477] Commission Green Paper, "Financial Services—Meeting Consumers' Expectations", COM(96) 209; Communication from the Commission, "Financial Services—Enhancing Consumer Confidence", COM(97) 309.
[478] For the Commission's initial proposals, see COM(98) 468 and COM(99) 385.
[479] Financial Services Distance Marketing Directive, para.3–152, n.426.
[480] *ibid.*, Art.1(1).
[481] *ibid.*, Art.2.
[482] *ibid.*, Art.3.
[483] *ibid.*, Art.3(1).
[484] *ibid.*, Art.3(2).

harmonisation, Member States may retain stringent requirements on the prior provision of information, provided that they comply with EU law.[485]

3–177 *Media for the provision of information*—Contractual terms and conditions and information must be communicated to the consumer on paper or on another durable media (such as floppy disks, CD-ROMs, DVDs or the hard drive of the consumer's computer, but not on a website) in good time before the consumer is bound by any distance contract or offer,[486] or, if the contract is concluded at the customer's request before that is done, immediately after the conclusion of the contract.[487] The consumer may at any time request a paper copy of the contract or change the means of distance communication.[488]

3–178 ***Right of withdrawal***—Consumers must have a period of at least 14 days to withdraw, without penalty, from the contract (which is extended to 30 days for life insurance and personal pension operations) without having to give any reason.[489] The supplier may not begin to perform the contract before expiry of the time limit for the exercise of the right of withdrawal without the consumer's express consent.[490] If the consumer exercises his right of withdrawal, he may be required to pay a sum compensating the supplier for the costs incurred and/or the services rendered prior to the exercise of the withdrawal.[491]

3–179 ***Other provisions***—The Financial Services Distance Marketing Directive contains a number of other provisions.

3–180 *Unsolicited communications*—As with the Distance Contracts Directive, Member States must prohibit the supply of financial services without prior request on the part of the consumer and exempt the customer from obligations to pay for such unsolicited services.[492] With respect to unsolicited communications, Member States must ensure that suppliers can only use distance communications if they have either obtained the consumer's consent or if the consumer has not manifestly expressed an objection.[493]

3–181 *No waiver of consumers' rights*—The consumer may not waive the rights conferred on him by national laws that transpose the Financial Services Distance Marketing Directive, and Member States must ensure that the consumer does not lose the protection granted by this Directive by virtue of the law of a third country being the applicable law of the contract, if the contract has a close connection with the territory of one or more Member States.[494]

3–182 *Sanctions*—Member States must provide for appropriate, effective, proportionate and dissuasive sanctions for a supplier's failure to comply with national implementing legislation.[495]

3–183 *Dispute resolution and consumer redress*—Adequate and effective judicial and administrative redress must be available to protect consumers' interests, including actions by public bodies,

[485] *ibid.*, Art.4(1) and (2).
[486] *ibid.*, Art.5(1).
[487] *ibid.*, Art.5(2).
[488] *ibid.*, Art.5(3).
[489] *ibid.*, Art.6.
[490] *ibid.*, Art.7(1).
[491] *ibid.* Member States may render withdrawal from an insurance contract free of charge to the consumer: *ibid.*, Art.7(2).
[492] *ibid.*, Art.9. This is without prejudice to the renewal of an existing contract, where that is permitted by national law.
[493] *ibid.*, Art.10. Communications by automatic calling machines and fax always require the prior consent of the consumer: *ibid.*, Art.10(1).
[494] *ibid.*, Art.12.
[495] *ibid.*, Art.11.

consumer organisations and professional organisations.[496] Member States must also put in place schemes for the out-of-court resolutions of consumer disputes and for providing redress to consumers.[497]

3–184 *Burden of proof*—Member States may place on the supplier the burden of proof to show that it has complied with its obligations to inform the consumer, to obtain the consumer's consent and to perform the contract.[498]

3–185 ***Implementation***—Member States were required to implement the Financial Services Distance Marketing Directive by October 9, 2004.[499]

3–186 **Framework Decision on Fraud and Counterfeiting**[500]—This Framework Decision requires Member States to treat as criminal offences a number of means of fraud and counterfeiting using non-cash means of payment. It covers the following misuses of "payment instruments" (*i.e.* credit cards or other cards issued by financial institutions, cheques and travellers' cheques): (i) theft of payment instruments; (ii) counterfeiting or falsification of payment instruments for fraudulent use; (iii) receiving, transporting or selling stolen or counterfeit payment instruments; and (iv) fraudulent use of stolen or counterfeit payment instruments. It also requires Member States to criminalise any theft or other property loss that is committed by means of using a computer to alter, delete or suppress computer data or otherwise interfere with the operation of a computer system. Finally, Member States must criminalise the fraudulent making, receiving, obtaining, sale or transfer of devices that are adapted for the commission of the criminal offences listed above.

3–187 **E-Commerce and Financial Services Communication**[501]—This Communication sets out a wide range of legislative and non-legislative measures that the Commission intends to adopt in order to complete the internal market in financial services. First, the Commission will develop a programme of convergence, covering contractual and non-contractual rules to implement the country of origin approach for all financial services sectors and forms of distance selling. This will involve: (i) legislation guaranteeing high levels of harmonised consumer protection relating to advertising, marketing and sales promotions (which has been implemented with the adoption of the Financial Service Distance Marketing Directive); (ii) legislation ensuring the convergence of sector-specific (*e.g.* banking, insurance, etc.) and service-specific (*e.g.* mortgage credit, consumer credit, etc.) national rules on information requirements to facilitate the easy comparison of prices and conditions; and (iii) an ongoing review of national rules on retail financial services contracts. Second, the Commission intends to take a number of non-legislative measures to increase consumer confidence in cross-border transactions and internet payments, by creating an EU-wide network to handle financial services complaints through third-party and alternative dispute resolution systems. With respect to internet payments, this Communication also supports the adoption of legislation granting consumers the right to a refund in the event of unauthorised transactions or non-delivery of goods or services.

[496] *ibid.*, Art.13.
[497] *ibid.*, Art.14.
[498] *ibid.*, Art.15.
[499] *ibid.*, Art.21(1).
[500] Council Framework Decision 2001/413 of May 28, 2001 combating fraud and counterfeiting of non-cash means of payment, O.J. 2001 L149/1.
[501] E-Commerce and Financial Services Communication, para.3–161, n.453.

3. Electronic money

3–188 Background—Initially, payment for goods and services obtained over the internet was made by traditional bank transfer. However, the development of e-commerce required faster means of payment and, as a result, credit cards and debit cards are now widely used as a means of payment on the internet. However, the use of credit cards on an open network like the internet raises issues of security (*e.g.* the interception of card numbers) and privacy (*e.g.* the tracking of customers' purchasing patterns). Although encryption can resolve some of these issues, these concerns have led to the creation of alternative means of payment that are specific to the internet.

3–189 Electronic accounts—Banks have developed electronic accounts ("e-accounts") for internet transactions. The user opens an e-account with a financial institution and receives an encrypted code, which identifies him in his internet transactions. The user transfers funds from his bank account to his e-account. When he wants to purchase an item on the internet, the user informs the seller of his code, which enables the seller to check the validity of the account with the relevant financial institution. The financial institution, which acts as an intermediary, then pays the seller and debits the buyer's e-account. The use of e-accounts thus avoids confidential information such as credit card numbers being communicated over the internet.

3–190 Electronic money—An innovative method of payment for transactions conducted on the internet is electronic money. Electronic money is digital data representing a certain monetary value. This monetary value is stored either on chips on bank cards or cards that are similar to phone-cards (*e.g.* the Proton system in Belgium and the Mondec system in the United Kingdom), or on computer software stored on a customer's PC that can be used to buy products or services over the internet. Customers wishing to use e-money must open an e-cash account with their bank or other e-money service provider in addition to their regular account. They will then be able to transfer amounts from their regular accounts to their e-cash accounts. Customers withdraw e-cash "coins" from their e-account and store them on their PC. Users can then pay with e-cash coins when purchasing goods or services over the internet. When the seller is paid with e-cash coins, he sends them to the bank for verification. The bank will then credit the amount on the e-cash account of the seller with the bank. For the time being, the e-cash system can only be used if the seller and the buyer have a bank account with the same bank. Electronic money has many characteristics of cash. The primary similarity is that no authorisation is required from a bank or third party to use electronic money, unlike with debit or credit cards. Another major similarity with cash is anonymity. Electronic money uses a system of blind signatures to avoid the bank being able to track the customer's spending. E-cash "coins" are not created at the bank but by the software installed on the customer's PC. Each e-cash "coin" has its own serial number and is sent to the bank in an encrypted digital envelope at the time the customer wishes to withdraw electronic money from his account. The bank validates the e-cash "coins" with digital stamps (without opening the digital envelope) and sends the e-cash "coins" back to the seller and debits the e-cash account of the customer. The bank is thus not able to recognise the e-cash "coins" it has stamped.[502] The use of these new payment techniques raises a number of legal issues, including: the legal status of electronic money and the relationship between the customer, the seller and the issuing bank; liability in the event of fraudulent use; consumer protection; and the legal status and supervision of users of

[502] See Abels, "Paying on the Net Means and Associated Risks" (1998) 3 *International Business Law Journal* 349; and Hance, para.3–001, n.1.

electronic money. This section reviews the EU regulatory initiatives that have been taken to address these issues.

3–191 ***Commission's Recommendation on Electronic Payment***—In 1997, the Commission adopted the Electronic Payment Recommendation, which concerned electronic payment instruments, with a view to promoting customer confidence and retailer acceptance of these instruments.[503] The Electronic Payment Recommendation is not binding on Member States, but the Commission indicated that it would propose appropriate binding legislation covering the issues dealt with in the Recommendation, if its implementation by the Member States was unsatisfactory. Member States were invited to take the necessary measures to implement the Electronic Payment Recommendation by December 31, 1998.

3–192 *Scope*—The Electronic Payment Recommendation applies to all transactions effected by means of an electronic payment instrument.[504] This covers remote access payment instruments of the e-account type, which allow payment at a distance through access, by way of a personal identification code, to funds held with an institution. It also covers electronic money instruments, which are reloadable payment instruments, consisting of a stored-value card or computer memory on which value units are stored electronically.[505] The term "issuer" is defined broadly to cover not only financial institutions but also any other institutions (such as supermarkets), which, in the course of their business, make available to their customers an electronic payment instrument pursuant to contracts concluded with them.

3–193 *Provision of information to consumers*—The Electronic Payment Recommendation provides for minimum requirements regarding the information to be provided to customers on the terms and conditions governing the issuance and use of electronic payment instruments. It also specifies the respective obligations and liabilities of the holder and of the issuer of electronic payment instruments.[506]

3–194 ***Electronic Money Institutions Directive***—In order to promote confidence and trust among businesses and consumers regarding the use of electronic money, the European Parliament and the Council have adopted the Electronic Money Institutions Directive.[507] This introduces a separate prudential supervisory regime for electronic money institutions, in order to secure the mutual recognition, authorisation and supervision of electronic money institutions on the basis of a single licence recognised throughout the EU.

3–195 *Scope*—An "electronic money institution" is defined as any institution, other than a credit institution as defined in the Credit Institutions Directive,[508] which issues means of payment in the form of electronic money.[509]

[503] Recommendation of July 30, 1997 concerning transactions by electronic payment instruments and in particular the relationship between the issuer and holder, O.J. 1997 L208/52.

[504] *ibid.*, Art.1.

[505] *ibid.*, Art.2.

[506] See Salaün, para.3–167, n.467, 19–31.

[507] Directive 2000/46 of September 18, 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, O.J. 2000 L275/39 ("Electronic Money Institutions Directive"). See Krueger, "E-money regulation in the EU", in Pringle and Robinson (eds.), *E-Money and Payment Systems Review* (2002), 239-251.

[508] Directive 2000/12 of March 20, 2000 relating to the taking up and pursuit of the business of credit institutions, O.J. 2000 L126/1, amended by Directive 2008/28 of September 18, 2000, O.J. 2000 L275/37 ("Credit Institutions Directive"). "Electronic money" is defined as monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less than the monetary value issued; and (iii) accepted as means of payment by undertakings other than the issuer.

[509] Electronic Money Institutions Directive, para.3–194, n.507, Art.1(3)(a).

3–196 *Activities of electronic money institutions*—The business activities of electronic money institutions must be limited to the issuing of electronic money and the provision of closely-related financial and non-financial services, such as administering electronic money and means of payment (excluding the granting of any form of credit).[510]

3–197 *Single passport*—Undertakings that issue electronic money but which do not wish to undertake the full range of banking activities nevertheless enjoy the benefits of being able to operate throughout the EU on the basis of authorisation in one Member State (the so-called "single passport") and so be on an equal footing with credit institutions.[511]

3–198 *Prudential regulation*—An alternative system of prudential regulation to that contained in the Credit Institutions Directive is provided for electronic money institutions, which includes requirements covering initial capital and ongoing own funds requirements, limitations on investments and sound and prudent operation.[512] The bearer of e-money may require the issuer to redeem it in coins and bank notes or by a transfer to a bank account free of charges other than those strictly necessary to carry out that operation. A minimum threshold for redemption may be stipulated in the contract between the issuer and the bearer, but the threshold may not exceed €10.[513]

3–199 *Grandfathering provisions*—Electronic money institutions that were operational before the implementation of the Electronic Money Institutions Directive (which was required by April 29, 2002) benefitted from "grandfathering" provisions and were presumed to be authorised in accordance with the Directive and thus benefit from mutual recognition. They then had six months to demonstrate compliance.[514]

3–200 ***Payment Services Directive***—The payment service markets of the Member States are organised separately, along national lines, and the legal framework for payment services is fragmented into 27 national legal systems. The proper operation of a single market in payment services is, however, considered vital in order to establish an internal market and actually enable the free movement of persons, goods, services and capital. The Payment Services Directive was adopted in order to establish at the EU level a modern and coherent legal framework for payment services.[515] The target is to make cross-border payments as easy, efficient and secure as domestic payments within a Member State. The Directive also seeks to improve competition by opening up payment markets to new entrants, thus fostering greater efficiency and cost-reduction. At the same time, the Directive provides the necessary legal platform for the Single Euro Payments Area (SEPA), which was created on January 28, 2008.

3–201 *Scope*—The Payment Services Directive deals with three major issues: it establishes who may provide "financial services"; it provides transparency requirements to ensure that payment service providers give requisite information to their customers as related to payments; and it sets

[510] *ibid.*, Art.1(5).
[511] *ibid.*, Art.2.
[512] *ibid.*, Arts.4, 5 and 7. These requirements are, however, lower than those applicable to credit institutions under the Credit Institutions Directive, para.3–194, n.508. Member States' regulatory authorities must verify compliance at least twice per year. *ibid.*, Art.6.
[513] *ibid.*, Art.3.
[514] *ibid.*, Arts.9 and 10.
[515] Directive 2007/64/EC of November 13, 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, O.J. 2007 L319/1. The Payment Services Directive was required to be implemented by the Member States by November 1, 2009.

out the relative rights and obligations of payment service providers and payment service users. The impact of this Directive with regard to electronic money seems to be rather limited. Its objective is to set rules on the execution of payment transactions in case the funds consist of electronic money.

3–202 *Exclusions*—Two specific aspects of electronic money are outside of the scope of the Directive: (i) rules on the issuing of electronic money; and (ii) the prudential regulation of electronic money institutions.[516] The Directive, however, provides that payment institutions are not allowed to issue electronic money.[517]Furthermore, payment services are not those connected to taking deposits or issuing electronic money but rather financial services supplied by legal persons through the EU.[518]

[516] Prudential regulation is dealt with in the Electronic Money Institutions Directive, para.3–194, n.507.
[517] *ibid.*, recital 9.
[518] *ibid.*, recital 10.