STUDY

DIRECTORATE GENERAL INTERNAL POLICIES OF THE UNION

EUROPEAN PARLIAMENT

Policy Department C
Citizens' Rights and Constitutional Affairs

STRENGTHENING SECURITY AND FUNDAMENTAL FREEDOMS ON THE INTERNET - AN EU POLICY ON THE FIGHT AGAINST CYBER CRIME

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

January 2009
PE 408.335

EN

PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Directorate General Internal Policies
Policy Department C
Citizens' Rights and Constitutional Affairs

STRENGTHENING SECURITY AND FUNDAMENTAL FREEDOMS ON THE INTERNET - AN EU POLICY ON THE FIGHT AGAINST CYBER CRIME

STUDY

Abstract:

This study examines the human rights aspects of the Internet, and looks in detail at the relevant criminal law rules of the Council of Europe and the EU. It also examines other aspects of the issue of cyber-crime, such as data protection rights, the EU's Safer Internet programme, child pornography, attacks on information systems, terrorism, racism and xenophobia.

The study concludes that the EU should set the following priorities in this area:

a) the adoption of a non-binding Internet Bill of Rights, a draft of which is presented in the Annex;

b) the development of EU substantive and procedural criminal law regarding cyber-crime; and

c) the development of EU operational action as regards cyber-crime.

PE 408.335

This study was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (**LIBE**).

This paper is published in the following languages: EN, FR.

Author: **Steve Peers (University of Essex)**

*Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (**CEPS**).*

Manuscript completed in **January 2009**

Copies can be obtained through:

Mr Alessandro DAVOLI
Administrator Policy Department C
Tel: 32 2 2832207
Fax: 32 2 2832365
E-mail: alessandro.davoli@europarl.europa.eu

Information on **DG IPOL publications**:

http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

http://www.ipolnet.ep.parl.union.eu/ipolnet/cms/pid/438

Brussels, European Parliament

TABLE OF CONTENT

I. INTRODUCTION

The EU and the Council of Europe have already between them adopted a number of different types of measures which directly or indirectly concern the issue of cyber-crime, and the protection of human rights in the Internet context. This study examines these measures in detail. But given the development of the Internet in recent years, this study also suggests further measures which the EU could consider taking in this area.

II. HUMAN RIGHTS PROTECTION ON THE INTERNET

Activity on the Internet is of course generally governed by the same human rights protections that derive, in their respective sphere of application, from national laws and constitutions, international human rights treaties (in particular the ECHR) and the general principles of Community law, along with the EU Charter of Fundamental Rights.

The most frequently invoked human rights in the context of the Internet are the right to privacy and the protection of personal data, along with the freedom of expression. Other rights which are particularly impacted by the Internet include the right to non-discrimination (in terms of access to the Internet and in terms of protection from, for instance, expressions of incitement to racial hatred and violence), the right to property (particularly intellectual property), the protection of human dignity (as regards, for instance the posting of abusive e-mails or content onto social networking sites) and the rights of the child – both to be protected from the risks of abuse on the Internet and also to have the right of access to the Internet as part of each child's education and social and cultural expression.

The drafting and promotion of an 'Internet Bill of Rights' could summarise these rights and draw them to the attention of Internet users, industry actors, the public sector (regulators, police officers, teachers, et al), relevant NGOs and the media. The Bill of Rights could be drawn up initially by the European Parliament, but could be open for signature and/or support by industry actors, NGOs, Member States, other EU institutions, media bodies and others. It could be endorsed and promoted on the websites of companies, NGOs, EU institutions and national public sector bodies.

The suggestion is not for a list of new rights or a legally binding instrument, but for a 'showcase' of relevant rights to inform the public about the application of human rights principles to the Internet.

As a drafting suggestion, a proposed Internet Bill of Rights appears in the Annex. The rights in the Bill of Rights have been excerpted directly from the most relevant provisions of the EU's Charter of Fundamental Rights, except for the final Article 14, which is a new provision relating to the content and interpretation of the rights (paragraph 1), based on the general provisions in Articles 51-54 of the Charter, and which confirms the existence of other rights (paragraph 2). The wording of the provision concerning consumer protection has also been reworded to refer to the Internet expressly (Article 13).

The draft Bill could be further amended, if desired, to refer in more detail to the context of the Internet, for example to the rules on confidentiality of communications, the prohibition of 'spam' and the protection of children.

III. CYBER-CRIME

1. Council of Europe Measures

1.1 Cyber-crime Convention

The principal Council of Europe measure relating to the issue of cyber-crime is obviously the Council of Europe Convention on Cyber-crime (ETS 185), opened for signature in 2001 and in force 1 July 2004. As of January 14 2009, the Convention has been ratified by 23 states in all, including 15 EU Member States and one non-member of the Council of Europe (the USA) and signed by a further 23 states, including the remaining 12 EU Member States - Austria, Belgium, Germany, Greece, Czech Republic, Ireland, Luxembourg, Malta, Poland, Portugal, Sweden and the UK – as well as three non-Members of the Council of Europe (Canada, Japan and South Africa).

Following definitions of the Convention's key terms in Article 1, the Convention sets out several categories of substantive crimes which parties must establish. First of all, there are six crimes relating to the confidentiality, availablity and integrity of computer systems: illegal access; illegal interception; data interference; system interference; and misuse of devices (Articles 2 to 6). States can limit (but not exclude entirely) their obligations to criminalise such acts, except as regards system interference. Next, there are two crimes related to computer systems, but not distinct to the online world: computer-related fraud and computer-related forgery (Articles 7 and 8). As regards forgery, parties may require a dishonest intent.

Third, there is one content-related offence, concerning child pornography. This concerns producing, offering or making available, distributing or transmitting, procuring, or possessing child pornography, via means of a computer system (Article 9(1)). Child pornography is defined as a minor 'engaging in sexually explicit conduct' (which is not further defined in the Convention itself), or a person appearing to be a minor engaging in such conduct, or 'realistic images representing a minor' engaging in such conduct (Article 9(2)). A 'minor' is a person below 18 years, except that a state can set a lower age limit of 16 or 17 (Article 9(3)). States may choose not to criminalise possession and procuring of child pornography, or to exclude liability when the images do not concern real children (Article 9(4)).

Finally, there is an obligation to criminalise specified infringements of copyright or related rights, 'where such acts are committed wilfully, on a commercial scale and by means of a computer system' (Article 10), although states need not impose criminal liability for such acts if they have another system of effective remedies for such breaches in place (Article 10(3)).

States are also obliged to criminalise the ancillary offences of aiding and abetting any of the main offences referred to (Article 11(1)), as well as attempts to commit most of those offences (Article 11(2)), except that parties can partly or wholly decline to impose any criminal liability for attempts (Article 11(3)).

Parties are obliged to extend their jurisdiction not only to their territory, to ships flying their flag and to aircraft registered on their territory, and also to their own nationals, if the act was criminal where it was committed or was committed outside the territorial jurisdiction of any state (Article 22(1)). However, reservations are permitted as regards the extension of jurisdiction beyond the territory (Article 22(2)). There is an obligation to 'extradite or prosecute' rule as regards a state's own nationals (Article 22(3)), and to consult where more than one party claims jurisdiction

(Article 22(5)), 'with a view to determining the most appropriate jurisdiction for prosecution'.

EU Member States which have ratified the Convention have made reservations in this area concerning: the definition of child pornography (Denmark, France, Hungary); the rules concerning illegal access (Finland, Lithuania, Slovakia); system interference (Slovakia); the criminalisation of attempts (Finland); and the jurisdictional rules (France, Latvia).

The Convention contains specific rules on procedural law (Articles 14-21). These rules are subject to general 'conditions and safeguards' under national law, which must include human rights safeguards and incorporate the principle of proportionality (Article 15(1)). These 'conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure' (Article 15(2)). Also, parties are obliged to consider the impact of these procedural rules upon the 'rights, responsibilities and legitimate interests of third parties', but this obligation applies '[t]o the extent that it is consistent with the public interest, in particular the sound administration of justice' (Article 15(3)).

The detailed obligations regarding procedural law concern: the expedited preservation of stored computer data; the expedited preservation and partial disclosure of traffic data; production orders relating to computer data; the search and seizure of stored computer data; the real-time collection of traffic data, and the collection of content data. However, reservations as regards the latter two issues are permitted where it is not technically possible to collect all such data (Articles 20(2) and 21(2)), and the obligation to collect content data only applies to 'a range of serious offences as defined by domestic law'. Also, parties can reserve their obligations to collect traffic data to specific categories of offences, as long as this list of offences is not shorter than the list of offences for which that state collects content data (Article 14(3)(a)). Parties can also reserve their obligations under these Articles where their national law does not provide for such measures to be taken against private computer systems (Article 14(3)(b)).

EU Member States which have ratified the Convention have made reservations in this area concerning the limitation of the collection of traffic data to certain offences (Bulgaria, Denmark, Finland), and as regards private computer systems (Finland). France has made a declaration specifying when the obligation to collect content data may apply in French law.

The Chapter on international cooperation (Articles 23-35) contains general rules relating to extradition and mutual assistance, as well as specific rules concerning requests for preservation of stored computer data, the expedited disclosure of stored traffic data, access to stored computer data, the real-time collection of traffic data or the interception of content data. Parties must also establish a '24/7' network to assist with investigations and prosecutions.

The Convention contains a general authorisation for parties to apply particular rules among themselves, with no specific reference to the EC or EU (Article 39(2)):

> If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that

agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

1.2 Protocol to the Convention on Cyber-crime

The Protocol (ETS 189) was opened for signature in 2003 and entered into force on 1 March 2006. It has been ratified by 21 states, and signed by 13 states, as of January 14 2009. It has been ratified by 6 EU Member States - Cyprus, Denmark, France, Latvia, Lithuania and Slovenia – and signed by 13 Member States – Austria, Belgium, Estonia, Finland, Germany, Greece, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania and Sweden. Eight Member States have not signed the Protocol - Bulgaria, the Czech Republic, Hungary, Ireland, Italy, Slovakia, Spain and the UK.

The Protocol entirely concerns the issue of substantive criminal law as regards 'racist and xenophobic material' (as defined in Article 2(1) of the Protocol, discussed further below). It requires the parties to ensure that four separate acts are criminalised within their domestic law: dissemination of such material through a computer system (Article 3); threatening, via a computer system, the commission of a serious criminal offence against a group defined by race, at al or religion (Article 4); an insult against a person or group or racial, religious, et al grounds, through a computer system (Article 5); and a denial, gross minimisation, approval or justification of genocide or crimes against humanity as defined in the Protocol, through a computer system (Article 6). Parties must also criminalise aiding or abetting any of these offences (Article 7).

However, parties are entitled to maintain reservations on several of these Articles, discussed further below.

1.3 Convention on the Prevention of Terrorism

This Convention (ETS 196, 2005), has been ratified by 15 states and signed by a further 28 states, as of January 14 2009. Among EU Member States, 7 have ratified it (Bulgaria, Denmark, Finland, France, Poland, Romania and Slovakia) and 19 have signed it (all remaining Member States except the Czech Republic). The Convention is open for signature by the EC, but the Community has not signed it. The Council of Europe Convention on the prevention of terrorism entered into force in June 2007.

The core of the Convention requires states to criminalise three types of act which could be committed offline as well as online, but which in practice are often committed online. These three offences are: the 'public provocation to commit a terrorist offence', as defined in Article 5; 'recruitment for terrorism', as defined in Article 6; and 'training for terrorism', as defined in Article 7. Article 8 of the Convention specifies that for any of these acts to constitute an offence, 'it shall not be necessary that a terrorist offence be actually committed'.

States must also criminalise participating as an accomplice in such offences, organising and directing others to commit them, contributing to their commission via means of a group of persons, and attempting to commit them (Article 9), although the obligation to criminalise attempts does not apply to the 'public provocation' offence. Such criminal sanctions are subject to human rights obligations and the principle of proportionality, and 'and should exclude any form of arbitrariness or discriminatory

or racist treatment' (Article 12). A 'terrorist offence' is defined by reference to the ten international conventions listed in the Appendix to the Convention (Article 1(2)).

Parties are obliged to extend their jurisdiction to their territory, as well as to ships flying their flag and to aircraft registered on their territory, and to acts committed by their own nationals (Article 14(1)). States *may* also exercise jurisdiction in a number of other cases (Article 14(2)). There is an obligation to consult where more than one party claims jurisdiction (Article 14(5)), 'with a view to determining the most appropriate jurisdiction for prosecution'. There is also a strong 'extradite or prosecute' rule (Article 18). The 'political offence' exception which is traditionally applicable to international criminal cooperation must be abolished as regards the crimes defined in the Convention, although parties are allowed to maintain a reservation in order to continue to apply it (Article 20). There is no obligation to extradite or provide mutual assistance 'if the requested Party has substantial grounds for believing that the request for extradition for offences [in the Convention]… or for mutual legal assistance with respect to such offences has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin or political opinion or that compliance with the request would cause prejudice to that person's position for any of these reasons' (Article 21(1)). There is also no obligation to extradite if the person concerned would face a real risk of torture or other inhuman or degrading treatment (Article 21(2)), or would face the death penalty or life imprisonment, if the requested state does not impose life imprisonment as a penalty (Article 21(3)).

Finally, the EU has insisted upon a 'disconnection' clause (Article 26(3)):

> Parties which are members of the European Union shall, in their mutual relations, apply Community and European Union rules in so far as there are Community or European Union rules governing the particular subject concerned and applicable to the specific case, without prejudice to the object and purpose of the present Convention and without prejudice to its full application with other Parties.

The explanatory report refers (at para. 272) to a declaration made by the Community and the Member States upon adoption of the Convention:

> The European Community/European Union and its Member States reaffirm that their objective in requesting the inclusion of a "disconnection clause" is to take account of the institutional structure of the Union when acceding to international conventions, in particular in case of transfer of sovereign powers from the Member States to the Community.
>
> This clause is not aimed at reducing the rights or increasing the obligations of a non-European Union Party vis-à-vis the European Community/European Union and its Member States, inasmuch as the latter are also parties to this Convention.
>
> The disconnection clause is necessary for those parts of the Convention which fall within the competence of the Community/Union, in order to indicate that European Union Member States cannot invoke and apply the rights and obligations deriving from the Convention directly among themselves (or between themselves and the European Community/Union). This does not detract from the fact that the Convention applies fully between the European Community/European Union and its Member States on the one hand, and the other Parties to the Convention, on the other; the Community and the European

> Union Members States will be bound by the Convention and will apply it like any Party to the Convention, if necessary, through Community/Union legislation. They will thus guarantee the full respect of the Convention's provisions vis-à-vis non-European Union Parties.

The report goes on to state that '[a]s an instrument made in connection with the conclusion of a treaty, within the meaning of Article 31, para. 2(b) of the Vienna Convention on the Law of Treaties, this declaration forms part of the "context" of the Convention.' It also notes (at para. 273) that the EC 'would be in a position to provide, for the sole purpose of transparency, necessary information about the division of competence between the Community and its Member States in the area covered by the present Convention, inasmuch as this does not lead to additional obligations placed on the Community.' It should be noted, however, that as noted above, the EC has not signed the Convention, and the Commission has not proposed that it do so.

When ratifying the Convention, Denmark reserved the right not to abolish the 'political offence' exception as regards the 'public provocation to commit terrorism', including in connection with ancillary offences. Hungary issued a declaration interpreting Article 5 of the Convention as regards the definition of 'public provocation'.

1.4 Convention on the protection of children against sexual exploitation and sexual abuse

This Convention (ETS 201, 2007) has been signed by 20 EU Member States and 13 non-Member States, but is not yet in force. The Convention is also open to signature and conclusion by the EC, but the EC has not signed it. It contains several provisions relevant to cybercrime. First of all, Member States are obliged to criminalise 'child pornography' offences as defined in Article 20(2) of the Convention. These offences entail, intentionally and 'without right', producing, offering or making available, distributing or transmitting, procuring, or possessing child pornography, or 'knowingly obtaining access, through information and communication technologies, to child pornography' (Article 20(1); the other offences can equally be committed online or offline). Parties may choose not to apply the latter offence (Article 20(4)), or not to criminalise the offences of producing and possessing child pornography where the images do not concern a real child, or which concern children who have reached the age of sexual consent but who produce and possess images for their own private use (Article 20(3)).

As compared to the relevant provisions of the cyber-crime convention, this Article is not limited solely to computer systems. The offence of obtaining access is also new as compared to that convention. A 'child' under the children Convention is any person under 18 years old (Article 3(a)), whereas the cyber-crime convention permitted the age to be lowered to 16 or 17 as regards child pornography (Article 9(3), cyber-crime Convention). The childrens' Convention contains a more precise definition of child pornography, which does not expressly refer to persons who *appear* to be minors. As for reservations, the childrens' Convention permits a general reservation as regards the new offence of online access, but otherwise the possibility for reservation is more limited: the cyber-crime convention permits general reservations as regards either the procurement or possession offences, or material that

does not involve actual children, but the children's convention permits reservations only as regards production or possession, and only in cases involving either material that either does not concern a real child or which is produced by minors above the age of sexual consent for their own purposes. So States which ratify the childrens' convention can no longer refrain from criminalising procurement of child pornography, and can only refrain from criminalising possession in very specific circumstances.

The Convention also sets out criminal offences relating to sexual abuse of children (Article 18), child prostitution (Article 19), the participation of children in pornographic performances (Article 21), and the corruption of children (Article 22), but such offences can obviously only be committed offline (note that the explanatory report to the Convention states that Article 21 'is intended to deal essentially with organised live performances of children engaged in sexually explicit conduct': para. 147).

Finally, the Convention also includes a 'grooming' offence. States must criminalise 'the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age' of sexual consent, in order to engage in sexual activities or to produce child pornography, 'where this proposal has been followed by material acts leading to such a meeting' (Article 23). No reservations to this Article are permitted.

States must also criminalise the aiding and abetting of such offences and attempts to commit them, but are permitted reservations on the obligation to criminalise attempts to commit the grooming and corruption offences, aspects of the 'participation' offence, and most child pornography offences (Article 24).

It should be noted that according to the explanatory report to the Convention, 'the negotiators did not consider it appropriate to introduce into the Convention provisions concerning awareness or ignorance, by the alleged perpetrator of the offence, of the victim's age. This question is a matter for the legislation and case-law of each Party, therefore' (para. 115). The report also states that 'the negotiators acknowledged that in certain circumstances where minors commit offences (such as, for example, where they produce child pornography among themselves and for their own private use but subsequently distribute those images or make them available on the Internet), there may be more appropriate methods of dealing with them and that criminal prosecution should be a last resort' (para. 116). Nevertheless, the Convention requires States to criminalise such wider circulation in such cases.

As regards specific aspects of substantive law, the explanatory report states that the 'child pornography' offence in the Convention 'is not restricted to child pornography committed by the use of a computer system. Nevertheless, with the ever-increasing use of the Internet this is the primary instrument for trading such material. It is widely believed that such material and on-line practices play a role in supporting, encouraging or facilitating sexual offences against children' (para. 134). The report further clarifies that '[m]aking available' is intended to cover, for instance, the placing of child pornography on line for the use of others by means of creating child pornography sites. This paragraph also intends to cover the creation or compilation of hyperlinks to child pornography sites' (para. 136). Furthermore, the term 'transmitting' covers '[s] ending child pornography through a computer system to another person' (para. 137). Procurement includes 'downloading computer data'

(para. 138). Possession includes material 'stored in a computer system' (para. 139). There is also a detailed description of the offence of online access (para. 140):

> It is intended to catch those who view child images on line by accessing child pornography sites but without downloading and who cannot therefore be caught under the offence of procuring or possession in some jurisdictions. To be liable the person must both intend to enter a site where child pornography is available and know that such images can be found there. Sanctions must not be applied to persons accessing sites containing child pornography inadvertently. The intentional nature of the offence may notably be deduced from the fact that it is recurrent or that the offences were committed via a service in return for payment.

The report also includes explanations of the term 'without right' and of the definition of 'pornography', and of the possibility of reservations.

Parties are obliged to extend their jurisdiction not only to their territory, to ships flying their flag and to aircraft registered on their territory, but also to apply a wide form of the 'active personality' principle, as they are obliged to extend jurisdiction to their own nationals and habitual residents who commit the offences set out in the Convention, wherever those offences are committed (Article 25(1)). However, reservations are permitted as regards the extension of such jurisdiction to habitual residents (Article 25(3)). Parties must also 'endeavour' to take measures to assert a wide form of 'passive personality' jurisdiction, as regards both their nationals and their habitual residents (Article 25(2)). Parties are obliged to waive the 'dual criminality' principle as regards producing child pornography (Article 25(4)) and aspects of participation in pornographic performances, and must also waive the requirement of a complaint from the victim regarding those particular offences, or a denunciation from the state where those offences were committed, before the active personality jurisdiction can be asserted (Article 25(6)). There is an obligation to consult where more than one party claims jurisdiction (Article 25(8)), 'with a view to determining the most appropriate jurisdiction for prosecution'. There is also an 'extradite or prosecute' rule as regards a state's own nationals (Article 25(7)).

The Convention also includes rules regarding corporate liability, the recognition of previous convictions, and aggravating circumstances, as well as a number of rules concerning investigations and procedural law. In particular there are detailed rules concerning the protection of victims, the initiation of prosecutions, the statute of limitations, interviews with children, and criminal court proceedings involving children. States must store records on the identity and genetic heritage (DNA) of persons convicted of offences pursuant to the Convention, and make such information available to other parties' authorities.

Finally, there is a general 'disconnection' clause in the Convention as regards EC/EU Member States (Article 43(3)):

> Parties which are members of the European Union shall, in their mutual relations, apply Community and European Union rules in so far as there are Community or European Union rules governing the particular subject concerned and applicable to the specific case, without prejudice to the object and purpose of the present Convention and without prejudice to its full application with other Parties.

This clause is identical to the disconnection clause in the Convention on the prevention of terrorism. The Community and its Member States made the same declaration as regards that other Convention (see para. 279 of the explanatory report on this Convention), and the report to this Convention similarly mentions that the Community could provide a clarification of competences (see para. 280 of the explanatory report). Again, as noted above, the EC has not signed the Convention, and nor has the Commission proposed that the Community sign it.

2. EC and EU measures

2.1 Substantive Law – Third Pillar Measures

2.1.1. Attacks on information systems

The first substantive EU law measure worth mentioning is the Framework Decision concerning attacks on information systems (OJ 2005 L 69/67). The Framework Decision requires States to establish three criminal offences: illegal access, illegal system interference and illegal data interference. All three offences are wider than the cyber-crime Convention in that the Convention only applies to 'computer systems', which it defines as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data' (Article 1(a) of the Convention). On the other hand the Framework Decision applies to *information* systems, which are defined as 'any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of *computer* data, *as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance*' (Article 1(a) of the Framework Decision; the words in italics are different from the Convention). The definition of 'computer data' is, however, identical in both measures (Article 1(b) of both the Framework Decision and the Convention).

As for the three specific offences, the offence of 'illegal access' is described identically, leaving aside the difference in scope as regards 'computer systems' and 'information systems'' (Article 2(1) of the Framework Decision; Article 2 of the Convention). The Framework Decision implicitly does not require criminalisation of 'minor' cases, and expressly permits Member States only to criminalise acts which were 'committed by infringing a security measure' (Article 2(2)).

Next, the offence of 'system interference' is described largely identically (Article 3 of the Framework Decision; Article 5 of the Convention), again leaving aside the difference in scope. However, the Framework Decision refers to the *interruption* of, as well as the serious hindering of, a computer system, and furthermore refers to 'rendering inaccessible' computer data. Again there is an implicit power for Member States not to criminalise minor cases.

Third, the offence of 'data interference' is the same, again leaving aside the difference in scope, and again with the addition of 'rendering inaccessible' computer data in the Framework Decision (Article 4 of the Framework Decision; Article 4 of the Convention). While the Framework Decision implicitly permits Member States not to criminalise minor cases, the Convention expressly permits parties not to criminalise cases unless they result in 'serious harm' (Article 4(2) of the Convention).

The Framework Decision does not address the closely related offences of illegal interception of data (Article 3 of the Convention) and misuse of devices (Article 6 of the Convention). Nor does it address the 'computer-related offences' of fraud and forgery via means of computers (Arts. 7 and 8 of the Convention). Both measures require States to impose liability for aiding and abetting and attempts, but with options to not criminalise attempts to commit illegal data access (Article 5 of the Framework Decision; Article 11 of the Convention).

As for jurisdiction, the Framework Decision requires Member States to assert jurisdiction where an act occurs in whole or part on their territory, was committed by their nationals (without qualification) or was committed for the benefit of a legal person with its head office in their territory (Article 10(1)). However, Member States can disapply all except territorial jurisdiction (Article 10(5)). The Framework Decision expressly specifies that territorial jurisdiction applies where:

> (a) the offender commits the conduct when physically present on its territory, whether or not the offence involves material hosted on an information system on its territory; or
>
> (b) the conduct involves material hosted on an information system in its territory, whether or not the offender commits the offence when physically present in its territory (Article 10(2)).

In contrast, the cyber-crime Convention requires parties to establish jurisdiction over acts on their territory, on board ships flying their flag or aircraft registered with them, and by their nationals subject to certain conditions (Article 22 of the Convention) but parties can enter reservations as regards all of these obligations except as regards territorial jurisdiction. So the position is very similar under the two measures, except for the clarification of territorial jurisdiction under the Framework Decision.

The Commission's proposal (COM (2002) 173) made clear that the Framework Decision did not address issues within the scope of EC law, in particular 'access to / disclosure of personal data, secrecy of communications, security of processing of personal data, electronic signatures or intellectual property violations and it does not prejudice the Directive 98/84/EC on the legal protection of services based on, or consisting of conditional access'. There are no criminal law obligations relating to such measures, but a proposal related to intellectual property is discussed further below.

The Commission has argued that in light of the Court of Justice jurisprudence on the scope of the EC's powers regarding criminal law, the Framework Decision should have been partly or wholly replaced by a Community law act COM (2005) 583). However, the Commission has not tabled any proposal to this effect. It has announced its intention to propose amendments to the Framework Decision in 2009, concerning 'in particular "botnets" and other instruments used to launch criminal attacks at a large scale' (see the Commission's 2009 work programme, COM (2008) 712).

2.1.2. Sexual exploitation of children and child pornography

Next, the EU has addressed the issue of sexual offences involving children in the Framework Decision on the sexual exploitation of children and child pornography (OJ 2004 L 13/44). This measure, which post-dates the cyber-crime Convention but pre-

dates the Council of Europe convention on childrens' protection, requires EU Member States to criminalise child pornography (Article 3) and child prostitution (Article 2). The latter offence can only be committed offline. As for the child pornography offence, Member States are obliged to criminalise the production, distribution, dissemination or transmission, supplying or making available and acquisition or possession of child pornography (Article 3(1)). The obligation applies regardless of any connection to a computer system. The Framework Decision defines 'child' as any person under eighteen (Article 1(a)), and also contains a definition of 'child pornography' (Article 1(b)), which applies also to material involving adults who appear to be children (Article 1(a)(ii)), and 'realistic images of a non-existent child' (Article 1(a)(iii)).

Member States may exempt from liability all cases where the real person involved in material was in fact an adult (Article 3(2)(a)). They may also exempt from liability all cases of production or distribution, dissemination or transmission, where the material is produced by persons over the age of sexual consent for their own private use, with the proviso that '[e]ven where the existence of consent has been established, it shall not be considered valid, if for example superior age, maturity, position, status, experience or the victim's dependency on the perpetrator has been abused in achieving the consent' (Article 3(2)(b)). Finally, they may exempt from liability all cases involving material relating to non-existent children, 'where it is established that the pornographic material is produced and possessed by the producer solely for his or her own private use', provided that no child pornography or material concerning adults appearing to be children was used to produce it, if there is no risk of further dissemination (Article 3(2)(c)).

Member States are also obliged to criminalise the instigation and aiding and abetting of all offences (Article 4(1)), and the attempts to commit all offences, except for attempts to possess or to supply or make available child pornography (Article 4(2)). Member States must provide for the possibility of imposing a sentence of at least one to three years for offences described by the Framework Decision, and for additional penalties of at least five to ten years in 'aggravating' circumstances (Article 5). However, they may impose non-criminal penalties in the cases of 'virtual' child pornography (Article 5(4)).

Member States must establish jurisdiction where the offence was committed wholly or partly within its territory, where the offender was one of its nationals, or where the offence was committed for the benefit of a legal person on national territory (Article 8(1)), although a Member State may deicide not to apply the latter two obligations (Article 8(2)). Each Member State must also 'ensure that its jurisdiction includes situations where an offence … is committed by means of a computer system accessed from its territory, whether or not the computer system is on its territory' (Article 8(5)). Member States are also obliged to permit the prosecution of at least the most serious offences after the victim has reached the age of majority (Article 8(6)).

As compared to the cyber-crime convention, the Framework Decision applies to all children under the age of 18, with no possibility to lower the age limit (cf. Article 9(3) of the Convention). Also, the Framework Decision is not limited to online activity. The Framework Decision also applies to 'dissemination' (not mentioned in the Convention), as well as to 'supplying' and 'acquiring' child pornography rather than 'offering' and 'procuring' it respectively. The Framework Decision's definition of 'child pornography' follows that in the Convention (Article 9(2)), with some

additional words in the former measure further defining 'sexually explicit conduct'. There is no general power under the Framework Decision to refrain from criminalising the procuring (ie acquisition) or possession of child pornography (cf Article 9(4) of the Convention), while the power to refrain from criminalising material related to 'virtual' children is confined to a particular case. However, the power to refrain from criminalising material related to adults appearing to be children is fully retained, and there is an additional possibility to refrain from criminalising material produced by children over the age of sexual consent for their private use.

The Framework Decision obliges Member States to criminalise aiding and abetting and inciting all offences, and attempting to commit some child pornography offences, but not attempting to supply, make available, acquire or possess child pornography (Article 4). This matches the Convention against cyber-crime, except that the latter does not apply to instigation, and also permits parties not to criminalise attempts relating to any aspect of child pornography (Article 11 of the Convention).

On other issues, the Framework Decision contains a general obligation to take jurisdiction over acts committed by a state's nationals, whereas the cyber-rcime Convention sets out only a qualified obligation; but both measures permit states not to apply such obligations. The cyber-crime Convention requires the application of jurisdiction to ships and aircraft connected to a Member State, but this is surely of limited relevance in practice, and states may refrain from applying these obligations in any case. The Framework Decision, unlike the cyber-crime Convention, does have a highly relevant clause regarding jurisdiction by means of computer systems accessed from the territory. The Framework Decision expressly applies the jurisdiction to acts taking place partly in the territory.

Comparing the Framework Decision to the childrens' Convention, there is no 'grooming' offence in the Framework Decision. As for the child pornography offence, the childrens' convention and the Framework Decision both apply to online and offline activity. They also have the same definition of 'child' (anyone under 18). There are the same minor differences as regards the wording of the core offences (ie, 'dissemination' is mentioned in the Framework Decision, but not the Convention; the Framework Decision refers to 'supplying' and 'acquiring' child pornography rather than 'offering' and 'procuring' it respectively). The bigger difference is that the Framework Decision does not contain the online access offence. The Convention contains similar wording to the Framework Decision as regards the extended definition of 'child pornography', but refers generally to the visual depiction of children ('any material that visually depicts a child…'), rather than the three categories (real children, adults appearing to be children and virtual children) referred to in the Cyber-crime convention and the Framework Decision.

Comparing the possible reservations, the childrens' Convention contains an unqualified possibility of not criminalising images of 'virtual' children as regards production and possession, whereas the Framework Decision is more qualified, but applies to all offences. Both measures permit a reservation as regards the possession and production of material by children above the age of sexual consent for their own use, except the EU measure contains a qualification about the possibility of the invalidity of consent. As regards the exception for images of adults in the Framework Decision, it is not clear whether the Convention applies to images of adults appearing to be children in any event.

As for inchoate offences, the childrens' Convention (Article 24), still does not apply to instigation, and obliges parties to criminalise aiding and abetting and attempts of the grooming and child pornography offences, except for the possibility not to criminalise attempts to commit the grooming offence and some of the child pornography offences. Parties must at least criminalise attempts to commit the offences of producing or distributing and transmitting child pornography. So the Framework Decision still sets a higher standard as regards the 'original' child pornography offences (ie apart from online access).

As regards jurisdiction, the childrens' Convention goes further than the Framework Decision by obliging parties to take jurisdiction against acts committed by their nationals, and moreover without any qualification (Article 25), whereas the Framework Decision allows Member States to derogate from this obligation. The Convention, unlike the Framework Decision, also applies to acts committed by residents, whereas the Framework Decision does not, although the Convention does permit a reservation on this point.

The draft EP report concerning the implementation of the Framework Decision (Angelilli report), recommends, inter alia, the following:

> (a) all Member States should sign and ratify the Cuncil of Europe childrens' Convention;
>
> (b) Member States should improve their legislation as regards variations in the age of sexual consent;
>
> (c) Member States should explicitly exclude a double criminality requirement for establishing jurisdiction;
>
> (d) Member States that have not yet entirely implemented the Framework Decision should be assisted in implementing it as soon as possible;
>
> (e) the monitoring of the implementation of the Framework Decision should be improved;
>
> (f) the Framework Decision should be revised to raise the level of protection to at least the level provided by the childrens' Convention and by 'tightening the focus on abuses related to the Internet and other communication technologies', including the following provisions:
>
> '– creation of national management systems for sex offenders that would include risk assessment, as well as intervention programmes to prevent or minimise the risk of repeat offences, and therapies available to sex offenders on a voluntary basis – criminalisation of *grooming* (solicitating children for sexual purposes) and the use of a definition of *grooming* based on the [childrens' Convention];
>
> – criminalisation of engaging in sexual activities with a child (below or above the age of sexual consent under national law) where use is made of coercion, force or threats, or abuse is made of a recognised position of trust, authority or influence over the child, including within the family, or abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence, or where money or other forms of remuneration or consideration is given as payment in exchange for the child engaging in sexual activities;
>
> – criminalisation of coercing a child into a forced marriage;
>
> – criminalisation of knowingly attending pornographic performances involving children and intentionally causing children to witness sexual abuse or activities;
>
> – criminalisation of paedophile chat rooms or Internet paedophile fora;

– allowing the national enforcement agencies to require Internet providers to block access to websites which are used to commit, or to advertise the possibility of committing, offences established in accordance with the Framework Decision;

– revision of Article 5(3) of the Framework Decision, which provides only a minimal basis for preventing convicted sex offenders from gaining access to children through employment or voluntary activities involving regular contact with children, inter alia by considering an obligation of Member States to ensure that applicants to certain posts working with children undergo criminal records checks, including setting up clear rules or guidelines for employers on their obligations in this regard;

– facilitating international cooperation by the use of the instruments provided for by the [childrens' Convention];

– releasing specific professional groups from the obligation of confidentiality, when a person encounters information about an offence established in accordance with the Framework Decision or has serious reason to believe that such an offence could have been committed, in cases where the information comes directly from a victim of sexual exploitation;

– obligation for professionals in contact with children to report situations where they have reasonable grounds for suspecting abuse;

– improving the identification of abused children through training of personnel having regular contact with them;

– facilitating the participation of children in court proceedings in order to avoid trauma by providing for specific arrangements on the way of collecting evidence from child victims through interviews; prohibiting advertisements encouraging activities which are likely to lead to the use of services that enable the commission of offences established in accordance with the Framework Decision;

– criminalisation of the instigation, aiding, abetting and attempting of all the offences established in accordance with the Framework Decision;

– expand the catalogue of aggravating circumstances in determining the sanctions in relation to offences established by the Framework Decision with a list of aggravating circumstances as established by [the childrens'] Convention;

– establish the exploitation of the superior position of an offender (in family, in education, in professional relations, when illegal migration takes place, etc.) as an aggravating circumstance;'

(g) the 'creation of a common European database that would collect images of child abuse'; and

(h) 'an action programme which would be aimed at providing the children who were identified as being sexually abused in such images with adequate protection and support'.

The Commission has announced its intention to propose amendments to the Framework Decision in 2009. This proposal will 'raise the level of protection for children currently granted… against sexual abuse, in particular under the form of sexual exploitation and child pornography. It is necessary to take account of new criminal phenomena and incorporate new provisions, thus bringing EU legislation in line with the highest international standards' (see the Commission's 2009 work programme, COM (2008) 712).

2.1.3 Terrorism

The EU's pre-existing Council Framework Decision on this issue, which obliges Member States to amend their criminal law as regards the definition of terrorism (OJ 2002 L 164/3), was amended in November 2008 in light of the 2005 Council of Europe Convention described above (OJ 2008 L 330/21; Member States must implement the new measure by 9 Dec. 2010). The amended Framework Decision inserts definitions of three further crimes into the original Framework Decision: 'public provocation to commit a terrorist offence', 'recruitment for terrorism' and 'training for terrorism' (amended Article 3(1) of the Framework Decision). Member States are obliged to ensure that these acts are considered as 'offences linked to terrorist activities' (amended Article 3(2)). It is also specified that for these acts to be punishable, 'it shall not be necessary that a terrorist offence be actually committed' (new Article 3(3)). This latter point corresponds to Article 8 of the Council of Europe Convention.

Furthermore, the 2002 Framework Decision has been amended to specify that there is an obligation to criminalise the aiding and abetting of such offences (amended Article 4(1)); but the revised Framework Decision does not require Member States to criminalise attempts and incitement of such offences (amended Article 4(2) and new Article 4(3)); the revised Framework Decision specifies only that Member States *may* criminalise attempts relating to training for terrorism and recruitment for terrorism (new Article 4(4)).

As compared to the Council of Europe Convention, the EU obligation to criminalise aiding and abetting could arguably be regarded as the equivalent of the Council of Europe obligation to criminalise participation as an accomplice, but the EU Framework Decision does not match the Council of Europe obligation to criminalise the organising and directing of others to commit these offences, the contribution to the commission of such offences via a group, or the attempt to commit two of these three offences. This is because the EU obligations relating to terrorist groups (Article 2 of the Framework Decision) apply only to 'terrorist offences', not to offences linked to terrorism. In any event, there are some differences between the EU and Council of Europe concept of a 'terrorist group' (compare Article 2(1) of the Framework Decision to Article 9(1)(c) of the Convention; the Convention does not in fact define 'terrorist group' as such), and the Council of Europe Convention refers to organising or directing others to commit the specified offences in the Convention (Article 9(1)(b)), while the Framework Decision refers to 'directing a terrorist group' (Article 2(2)(a)).

Moreover, there are differences between the EU and the Council of Europe measures as regards the underlying 'terrorist' offences that the new offences are linked to. As noted above, the Council of Europe Convention defines a 'terrorist offence' as an act banned by one of the ten UN treaties referred to in the Appendix to the Convention (Article 1(1) of the Convention). But the Framework Decision instead defines as terrorist offences eight specified acts (or the threat to commit them), committed in light of their particular nature and context and with a particular specified aim (Article 1(1) of the Framework Decision). There is obviously a large degree of overlap between the offences covered by the two measures, but it is not complete (for a comparison between UN terrorism measures and the original Framework Decision, see S. Peers, 'EU Responses to Terrorism', 52 ICLQ (2003) 227).

The core offence regarding recruitment for terrorism is also different, as the Convention requires that States criminalise 'solicit[ing] another person to commit or participate in the commission of a terrorist offence, or join[ing] an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group' (Article 5(1)), while the revised Framework Decision requires Member States to criminalise 'soliciting another person to commit one of the [terrorist] offences' referred to in the Framework Decision, or the direction of or participation in a terrorist group as defined in the Framework Decision (new Article 3(1)(b)). The EU does not require the criminalisation of the solicitation of participation *per se*, and the EU concept of participation in a terrorist group is more precisely but more broadly defined (see Article 2(2)(b) of the Framework Decision, which *inter alia* refers to 'criminal activities', not just 'terrorist offences').

There are also differences as regards jurisdiction. As noted above, the Convention (Article 14(1)) requires States to take jurisdiction as regards their territory, as regards an extended notion of territory (ships flying the flag of, and aircraft registered in, that State), as well as active personality jurisdiction (acts committed by nationals of the State). On the other hand, the Framework Decision also requires each Member State to take jurisdiction also as regards acts committed by its 'residents', where 'the offence is committed for the benefit of a legal person established in its territory' and where the offence is committed against the institutions or people of the Member State in question or against an institution of the European Union or a body set up in accordance with' the EU or EC Treaties and 'based in that Member State' (Article 9(1) of the Framework Decision).

It should be noted that, as regards the Convention, the territorial jurisdiction will apply to the place where the *linked* offence was committed, which may be separate from the place where the *main* offence would be committed (see the explanatory report to the Convention, para. 34: '…the place where such an offence would be committed is also irrelevant for the purposes of establishing the commission of any of the offences…'; see also paras. 79, 126 and 127 of the report.) Arguably the same rule is true of the Framework Decision. So, for example, a 'public provocation' in France to commit a 'terrorist' act in Iraq would be covered by the measures. If the reverse situation occurred (a 'public provocation' in Iraq to commit a 'terrorist' act in France), Member States would have to take jurisdiction under the Framework Decision (since this would surely qualify as an act 'against the institutions or the people of the Member State', under Article 9(1)(e)), but not necessarily under the Convention, where 'passive personality' jurisdiction is merely optional (Article 14(2)(a) of the Convention).

As for the safeguards in the two measures, the Convention specifies that States' obligations must be 'carried out while respecting human rights obligations, in particular the right to freedom of expression, freedom of association and freedom of religion, as set forth in, where applicable to that Party, the Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, and other obligations under international law' (Article 12(1)). It also specifies that the criminalisation obligations 'should furthermore be subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, and should exclude any form of arbitrariness or discriminatory or racist treatment' (Article 12(2)).

For its part, the amending Framework Decision states that it 'shall not have the effect of requiring Member States to take measures in contradiction of fundamental principles relating to freedom of expression, in particular freedom of the press and the freedom of expression in other media as they result from constitutional traditions or rules governing the rights and responsibilities of, and the procedural guarantees for, the press or other media where these rules relate to the determination or limitation of liability' (Article 2). The preamble to the amending measure also states that:

> (13) The Union observes the principles recognised by Article 6(2) of the EU Treaty and reflected in the Charter of Fundamental Rights of the European Union, notably Chapters II and VI thereof. Nothing in this Framework Decision may be interpreted as being intended to reduce or restrict fundamental rights or freedoms such as freedom of expression, assembly, or of association, the right to respect for private and family life, including the right to respect of the confidentiality of correspondence.
>
> (14) Public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism are intentional crimes. Therefore, nothing in this Framework Decision may be interpreted as being intended to reduce or restrict the dissemination of information for scientific, academic or reporting purposes. The expression of radical, polemic or controversial views in the public debate on sensitive political questions, including terrorism, falls outside the scope of this Framework Decision and, in particular, of the definition of public provocation to commit terrorist offences.
>
> (15) The implementation of the criminalisation under this Framework Decision should be proportional to the nature and circumstances of the offence, with respect to the legitimate aims pursued and to their necessity in a democratic society, and should exclude any form of arbitrariness or discrimination,

The original Framework Decision specifies that it 'shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union' (Article 1(2)). The preamble to the original Framework Decision specifies that:

> (10) This Framework Decision respects fundamental rights as guaranteed by the [ECHR] and as they emerge from the constitutional traditions common to the Member States as principles of Community law. The Union observes the principles recognised by Article 6(2) of the Treaty on European Union and reflected in the Charter of Fundamental Rights of the European Union, notably Chapter VI thereof. Nothing in this Framework Decision may be interpreted as being intended to reduce or restrict fundamental rights or freedoms such as the right to strike, freedom of assembly, of association or of expression, including the right of everyone to form and to join trade unions with others for the protection of his or her interests and the related right to demonstrate.

These safeguards apply equally to the amending measure.

2.1.4. Racism and xenophobia

The Protocol to the cyber-crime Convention relating to racism and xenophobia can be compared to the recent EU Council Framework Decision on the same issue (OJ 2008

L 328/55), adopted in November 2008. The Protocol and Framework Decision have different definitions of the key underlying offences. For the Protocol, '*"racist and xenophobic material"* means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors' (Article 2(1) of the Protocol). As noted above, parties are required to criminalise four separate acts: dissemination of such material through a computer system; threatening, via a computer system, the commission of a serious criminal offence against a group defined by race, at al or religion; an insult against a person or group or racial, religious, et al grounds, through a computer system; and a denial, gross minimisation, approval or justification of genocide or crimes against humanity as defined in the Protocol, through a computer system. Parties must also criminalise aiding or abetting any of these offences.

As noted above, a number of reservations are permitted. As regards the dissemination of racist or xenophobic material, parties may either exempt such material from criminal liability to the extent that the national principles concerning freedom of expression require this (Article 3(3)), or alternatively exempt from criminal liability material which 'advocates, promotes or incites *discrimination*' as distinct from hatred or violence, provided that other effective remedies are available' (Article 3(2); emphasis added). As for the requirement to criminalise racial insults, a party can decide either not to apply this provision at all (Article 5(2)(b)), or 'require that the offence…has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule' (Article 5(2)(a)). Finally, as regards denial of genocide, et al, a party can either again decide not to apply this provision at all (Article 6(2)(b)), or 'require that the denial or the gross minimisation…is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors' (Article 6(2)(a)). On the other hand, no reservation is permitted as regards the requirement to criminalise racial threats made through a computer system.

Of the EU Member States which have ratified the Protocol, Denmark has invoked all three reservations in order to announce that it may refrain in part or whole from establishing the offences referred to in Articles 3, 5 and 6 of the Protocol, while Lithuania has invoked the reservation permitted by Article 6(2)(a). France has issued a declaration stating its interpretation of Article 6.

For the Framework Decision, Member States must first establish as a criminal offence 'publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin' (Article 1(1)(a)), or the 'the commission of [such an act] by public dissemination or distribution of tracts, pictures or other material' (Article 1(1))(b)). As regards these crimes, Member States have an option to 'choose to punish only conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting' (Article 1(2)). The Framework Decision also states that the reference to 'religion' in the definition of the crimes 'is intended to cover, at least, conduct which is a pretext for directing acts against a group of persons or a member of such a group defined by reference to race, colour, descent, or national or ethnic origin' (Article 1(3)). This is quite similar to the reference to religion in the cyber-crime Protocol.

As compared to the Protocol, *promotion* and *advocacy* of violence or hatred is not covered by the Framework Decision, and there is no reference to discrimination. So the possible reservation as regards discrimination provided for in the Protocol is redundant as far as the Framework Decision is concerned (but see the discussion of EC measures below). The Framework Decision distinguishes between public incitement on the one hand, and dissemination on the other, while the Protocol concerns only dissemination; and the Framework Decision does not expressly cover insults or threats. But in some cases, the public incitement of hatred or violence covered by the Framework Decision would overlap with a threat or insult as defined by the Protocol. Most obviously, the Protocol limits its scope to online activity, while the Framework Decision does not.

As for the 'Holocaust denial' and similar crimes, the Protocol requires parties to criminalise 'distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court' if recognised by the parties. As noted above, parties can either again decide not to apply this provision at all, or require that the action 'is committed with the intent to incite hatred, discrimination or violence' on grounds of race, etc.

The Framework Decision applies to 'publicly condoning, denying or grossly trivialising' the Holocaust or similar crimes, 'directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group' (Article 1(1)(c) and (d)). Member States have an option under the Framework Decision to declare that they will only criminalise denying or grossly trivialising these crimes if they 'have been established by a final decision of a national court of this Member State and/or an international court, or by a final decision of an international court only' (Article 1(4)). They may also, as with the other crimes in the Framework Decision, 'choose to punish only conduct which is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting' (Article 1(2)).

Compared to the protocol, the Framework Decision does not permit an opt-out from this provision altogether. It also applies both to offline and online activity, whereas the Protocol only applies to online activity. Furthermore, it applies to a broader scope of denials than those cases where war crimes, et al have been established by international courts – although Member States have an option to limit its application to such cases. Again the Framework Decision does not apply to discrimination, only to hatred and violence; and it applies to measures likely to incite a response, whereas the Protocol applies to measures intended to incite a response. But this difference is undercut by the possibility to limit the application of the Framework Decision to conduct which threatens public order, or which is insulting, et al.

The Framework Decision, like the Protocol, applies to aiding and abetting all of the relevant offences (Article 2(2)). Unlike the Protocol, it also applies to instigation of the 'Holocaust denial' offences (Article 2(1)). Both measures specify, in slightly different terms, that they do not require States to act against fundamental principles of freedom of expression, but the EU measure refers only to exempting the media for liability as regards all of the crimes referred to (Article 7(2)), whereas the Protocol

refers to an exemption from the dissemination of racism and xenophobic material as regards the freedom of expression more generally.

The Protocol applies the same jurisdiction rules as the cyber-crime convention (Article 8(1) of the Protocol), with an option for parties to make the same reservations as regards the jurisdiction rules (see Article 12(2) of the Protocol). This means that States must establish jurisdiction over acts on their territory, on board ships flying their flag or aircraft registered with them, and by their nationals subject to certain conditions (Article 22 of the Convention) but parties can enter reservations as regards all of these obligations except as regards territorial jurisdiction. As for the Framework Decision, Member States must assert jurisdiction where an act occurs in whole or part on their territory, were committed by their nationals (without qualification) or was committed for the benefit of a legal person established in their territory (Article 9(1)). However, Member States can disapply all except territorial jurisdiction (Article 9(3)). So the position is the same as under the Protocol, except that the Framework Decision expressly specifies that territorial jurisdiction applies where:

> (a) the offender commits the conduct when physically present in its territory, whether or not the conduct involves material hosted on an information system in its territory; or
>
> (b) the conduct involves material hosted on an information system in its territory, whether or not the offender commits the conduct when physically present in its territory (Article 9(2)).

2.2 EC law – first pillar measures

Community law has not established any criminal law offences related to cyber-crime, as to date the Court of Justice jurisprudence has only clearly established the EC's criminal law competence related to the environment (Cases C-176/03 and C-440/05). To date, the question of whether the Community has criminal law competence in any other areas is open.

2.2.1 Intellectual property rights

In the specific area of intellectual property rights, the Commission has proposed a Directive that would establish criminal law obligations as regards 'all intentional infringements of an intellectual property right on a commercial scale' (Article 3, COM (2006) 168). This would apply to 'intellectual property rights provided for in Community legislation and/or national legislation in the Member States' (Article 1 of proposal). The proposal is not currently under discussion in the Council, although the EP has voted its first-reading opinion.

The Commission proposal could be compared to the obligation in the cyber-crime Convention to establish offences related to 'the infringement of copyright', as established under national law and pursuant to specified international conventions, 'with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system' (Article 10(1)), and of 'related rights' under the same conditions (Article 10(2)). A party can derogate from these obligations in 'limited circumstances, provided that other effective remedies are available and that such reservation does not

derogate from the Party's international obligations' under the specific treaties referred to (Article 10(3)).

2.2.2 Other measures

Other areas of Community law which are related to cyber-crime are the issue of race discrimination (as distinct from violence), which is the subject of Directive 2000/43, and data protection, which is the subject of Directive 95/46 and, as regards the telecommunications sector, Directive 2002/58 (OJ 2002 L 201/37). These acts do not establish criminal law obligations. If the Community does have criminal law powers in areas other than the environment where necessary in order to ensure effective enforcement of the rules it lays down (by analogy with the environmental law judgments referred to above), then it would be competent to establish criminal law penalties relating to race discrimination (to parallel aspects of the Protocol to the Cyber-crime Convention) and data protection law. The latter obligations could parallel in part the cyber-crime Convention offence of data interference (Article 4 of the Convention), although it should be noted that the obligation in the Convention is not limited to cases involving *personal* data, and the Directive applies not just to computer systems but to telecommunications networks more broadly. The specific provision of the e-privacy Directive involved concerns confidentiality of communications (Article 5), but the question might also be raised whether there should be criminal law obligations relating to data security (Article 4) and to unsolicited communications (Article 13(1) and (4)), at least in the most egregious cases of 'spam'. Criminal law obligations could also be attached to the equivalent provisions of the more general data protection Directive.

There is also a certain degree of overlap between the EC legislation prohibiting devices which ensure illicit access to various broadcasting or computer services (Directive 98/84, OJ 1998 L 320/54), and the criminalisation of the misuse of devices in the cyber-crime Convention (Article 6).

2.3 Procedural law

As regards the procedural law provisions of the Council of Europe Cyber-crime Convention, the EC Directive on data retention (Directive 2006/24, OJ 2006 L 105/54) is obviously relevant. As compared to Article 20 of the Convention, the Directive has a different definition of 'traffic data' (Article 2(b) of Directive; Article 1(d) of Convention); the Directive also applies to location data. However, there may be only a limited overlap between the two provisions, if any, since the Convention only applies to 'real-time' interception, while the Directive applies to retention for possible use later on. There is also a degree overlap as regards cases where the Convention applies to the preservation of stored computer data, which may include traffic data (Arts. 16 and 17 of the Convention).

As regards cross-border measures, there is likely to be a degree of overlap between the Convention's provisions on the expedited preservation of stored computer data (Article 29 of the Convention), and the EU's Framework Decision on the mutual recognition of orders freezing assets or evidence (OJ 2003 L 196/45).

2.4 Other EC and EU measures

The Community has recently adopted the most recent version of the 'Safer Internet' programme (OJ 2008 L 348/118), which has the goal of 'protecting children using the Internet and other communication technologies'. There is also an EC 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 (OJ 2006 L 378/72). The latter measure suggests in particular '(a) adopting a quality label for service providers, so that users can easily check whether or not a given provider subscribes to a code of conduct,' and '(b) establishing appropriate means for the reporting of illegal and/or suspicious activities on the Internet' (point 4), as well as referring to filtering systems, content labelling and age labelling (point 5).

As for the operational aspects of cyber-crime, there is a Council Recommendation on 24-hour contact points to combat cyber-crime (OJ 2001 C 187/5), which implements one of the provisions of the cyber-crime Convention (Article 35). Cyber-crime falls within the remit of both Europol and Eurojust. The October 2008 JHA Council adopted conclusions on the issue of cyber-crime, which called upon the Member States to set up alert platforms 'for the purpose of centralising alerts on offences noted on the Internet', and also recommended an EU platform hosted by Europol.

The Commission has suggested that an EU cyber-crime network could be set up (Communication on cyber-crime, COM (2007) 267). This would be comparable to the existing networks set up as regards other areas of crime (cf the anti-corruption network, OJ 2008 L 301/38 and the Decision establishing an asset recovery network, OJ 2007 L 332/103).

It should also be recalled that EU criminal law mutual recognition measures abolish dual criminality as regards 'computer-related-crime', although several measures provide for exceptions to abolish the dual criminality requirement, and most are subject to a threshold of a three-year penalty in the law of the issuing State. There are also varying exceptions to the obligation to recognise other Member States' decisions, in particular a territoriality exception which could be particularly relevant in the case of cyber-crime.

The relevant adopted measures are:

1) the Framework Decision on the European Arrest Warrant (OJ 2002 L 190/1), Article 2;
2) the Framework Decision on freezing orders (OJ 2003 L 196/45), Article 3;
3) the Framework Decision on financial penalties (OJ 2005 L 76/16), Article 5; there is no penalty threshold and dual criminality is also abolished as regards 'infringements of intellectual property rights' and penalties to enforce EC or EU law obligations;
4) the Framework Decision on confiscation orders (OJ 2006 L 328/), Article 6;
5) the Framework Decision on probation, et al (OJ 2008 L 337/102), Article 10; Member States may still retain dual criminality as an option (Article 10(4));
6) the Framework Decision on transfer of prisoners (OJ 2008 L 327/27), Article 7(4); Member States may still retain dual criminality as an option (Article 7(4)); and

7) the Framework Decision on the European Evidence Warrant (OJ 2008 L 350/72), Article 13; Germany will only abolish dual criminality to the extent that offences fall within the scope of the Framework Decision on attacks on information systems, or the core offences concerning the functioning of computer systems in the cyber-crime Convention (Article 23(4) and declaration).

It should also be recalled that cyber-crime offences will fall within the scope of the Schengen *ne bis in idem* rules (Arts. 54-58, Schengen Convention); these rules are particularly likely to be applicable in light of the cross-border nature of many cyber-crime offences. Furthermore, the ne bis in idem rule is a mandatory or optional exception to the application of the EU's various criminal law mutual recognition measures.

Finally, the Czech Presidency of the Council is planning to propose a Framework Decision imminently on the issue of preventing and settling conflicts of jurisdiction. Again, due to the cross-border nature of many cyber-crime offences, this proposal is likely to be particularly relevant to this area.

It might be considered that, given the complications that arise from overlapping jurisdiction in this area, the EU could consider further defining how the principle of territorial jurisdiction applies as regards computer-related offences in particular.

IV. CONCLUSIONS

This study has suggested that the following could be considered as priorities as regards EU action in the area of fundamental rights on the Internet and combating cyber-crime:

a) the adoption of a non-binding Internet Bill of Rights;

b) the possible alignment of EU substantive criminal law with the provisions of the relevant Council of Europe measures, in particular as regards offences relating to data protection rights (particularly data interception/communication confidentiality, data security and 'spam'), online fraud and forgery (for instance, 'phishing'), child pornography and the online 'grooming' of children for the purposes of committing sexual abuse;

c) adopting a measure establishing an operational network dealing with cyber-crime matters; and

d) the clarification of issues of territorial jurisdiction as regards cyber-crime issues.

ANNEX

Internet Bill of Rights

In the context of the Internet, the following rights must in particular be respected, observed and promoted:

Article 1

Human dignity

Human dignity is inviolable. It must be respected and protected.

Article 2

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 3

Protection of personal data

Everyone has the right to the protection of personal data concerning him or her.

Article 4

Freedom of expression and information

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.

Article 5

Freedom of the arts and sciences

The arts and scientific research shall be free of constraint. Academic freedom shall be respected.

Article 6

Right to property

Intellectual property shall be protected.

Article 7

Non-discrimination

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.

Article 8

Cultural, religious and linguistic diversity

The Union shall respect cultural, religious and linguistic diversity.

Article 9

Equality between women and men

Equality between women and men must be ensured in all areas.

Article 10

The rights of the child

1. Children shall have the right to such protection and care as is necessary for their well-being. They may express their views freely. Such views shall be taken into consideration on matters which concern them in accordance with their age and maturity.

2. In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.

Article 11

The rights of the elderly

The Union recognises and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life.

Article 12

Integration of persons with disabilities

The Union recognises and respects the right of persons with disabilities to benefit from measures designed to ensure their independence, social and occupational integration and participation in the life of the community.

Article 13

Consumer Protection

A high level of consumer protection shall be guaranteed as regards the Internet.

Article 14

General provisions

1. The content of these rights, including their field of application, their scope and interpretation (including any derogations and limitations on the rights), the level of protection guaranteed by these rights and the prohibition on abuse of these rights, shall be governed by the rules on the protection of human rights guaranteed by the constitutions of the Member States, international human rights treaties, including the European Convention on Human Rights, the general principles of Community law and the EU Charter of Fundamental Rights, or by other relevant rules of national, international, Community and Union law, in their respective fields of application.

2. This Bill of Rights is without prejudice to other rights applicable to the Internet, or rights applicable in other fields, guaranteed by the constitutions of the Member States, international human rights treaties, including the European Convention on Human Rights, the general principles of Community law and the EU Charter of Fundamental Rights, or by other relevant rules of national, international, Community and Union law, in their respective fields of application.