Council of Europe Conference of Ministers responsible for Media and Information Society

FREEDOM OF EXPRESSION AND DEMOCRACY IN THE DIGITAL AGE

OPPORTUNITIES, RIGHTS, RESPONSIBILITIES

Belgrade, 7-8 November 2013

Republic of Serbia
Ministry of Culture and Information

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MCM(2013)007

ONLINE FREEDOM OF EXPRESSION, ASSEMBLY, ASSOCIATION AND THE MEDIA IN EUROPE

REPORT

Ian Brown

University of Oxford, UK

Website: http://www.oii.ox.ac.uk/

E-mail: ian.brown@oii.ox.ac.uk

"The digital revolution has been good for freedom of expression because it has increased the diversity of voices in the public sphere.
The digital revolution has been good for freedom of information because it has made government documents and data directly accessible to more people and has fostered a culture that demands transparency from powerful institutions.
But the digital revolution has both revitalized and weakened freedom of the press."
Paul Starr[1]

This report provides an overview of recent challenges and threats to online freedom of expression, assembly, association and the media in Europe, and analyses the roles and responsibilities of State and non-state actors in protecting it. As well as research by the Council of Europe[2] and jurisprudence of the European Court of Human Rights (ECtHR),[3] it draws on surveys and analyses from institutions such as the Organisation for Security and Cooperation in Europe (OSCE) and European Commission, and the reports of the UN special mandate holders. A parallel report addresses Internet freedom issues relating to privacy and surveillance.

[1] An Unexpected Crisis: The News Media in Postindustrial Democracies, The International Journal of Press/Politics 17(2) p. 234, 2012

[2] Council of Europe, Protecting freedom of expression and information, http://hub.coe.int/protecting-freedom-of-expression-and-information

[3] ECtHR Research Division, Internet: case-law of the European Court of Human Rights, 2011; ECtHR Press Unit, New technologies factsheet, 2013; and relevant judgments and admissibility decisions

Table of contents

Freedom of expression

The ECtHR famously found in its *Handyside* decision that: "The Court's supervisory functions oblige it to pay the utmost attention to the principles characterising a 'democratic society'. Freedom of expression constitutes one of the essential foundations of such a society, one of the basic conditions for its progress and for the development of every man."[4]

Internet users' right to access and impart information and content of their choice is protected by Article 10(1) of the European Convention on Human Rights, "regardless of frontiers", with the limitations in Article 10(2) tested strictly: "every 'formality', 'condition', 'restriction' or 'penalty' imposed in this sphere must be proportionate to the legitimate aim pursued."[5] Political expression – even when exaggerated or virulent – is strongly protected.[6]

The Internet's global reach can strengthen State interests in proportionate measures to restrict the right to impart information – but also provide an important means of expression when other restrictions are imposed.[7] Individual rights "must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."[8]

Universal access and network neutrality

Having access to the Internet is the first step for individuals to benefit from its potential to support their freedom of expression. The Committee of Ministers has declared that: "Member states should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price."[9] The UN Special Rapporteur on freedom of opinion and expression, Frank La Rue, has stated: "ensuring universal access to the Internet should be a priority for all States".[10] The EU's statistical agency Eurostat found that in 2012, 72% of EU households have broadband Internet access, but some eastern European countries have lower levels of household access (with Greece, Bulgaria and Romania at 50% or 51% - although Romania has a significant number of households with modem or ISDN access). Eurostat also found that 39% of EU-resident individuals use mobile devices such as smartphones to go online.[11]

---

[4] Handyside v. the United Kingdom, Series A no. 24, § 49, 7.12.1976

[5] *Ibid*.

[6] *Renaud v. France*, no. 13290/07, § 38, 25.2.2010

[7] *Mouvement Raëlien Suisse v. Switzerland*, no. 16354/06, §§ 54-58, 13.1.2011

[8] *K.U. v. Finland*, no. 2872/02, 2.12.2008

[9] *Declaration on freedom of communication on the Internet*, Adopted on 28 May 2003 at the 840th meeting of the Ministers' Deputies

[10] A/HRC/17/27 § 85, 16.5.2011

[11] Data tables available from http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/

The Court has already found that "Article 10 also applies to the various forms and means in which [information] is transmitted and received".[12] It has noted that: "The right to Internet access is considered to be inherent in the right to access information and communication protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens. It can therefore be inferred from all the general guarantees protecting freedom of expression that a right to unhindered Internet access should also be recognised."[13]

This is already the explicit constitutional situation in two of the Council of Europe's member States. The French constitutional council in 2009 found that access is a right guaranteed by the 1793 *Déclaration des droits de l'homme et du citoyen*,[14] while the Greek constitution states that everyone has a right to participate in the information society, with the State obliged to facilitate "access to electronically transmitted information, as well as of the production, exchange and diffusion thereof".[15] England and Wales' Court of Appeal has found that:

> *"A blanket prohibition on computer use or internet access is impermissible. It is disproportionate because it restricts the defendant in the use of what is nowadays an essential part of everyday living for a large proportion of the public, as well as a requirement of much employment. Before the creation of the internet, if a defendant kept books of pictures of child pornography it would not have occurred to anyone to ban him from possession of all printed material. The internet is a modern equivalent."*[16]

Civil society groups have suffered technical attacks on their websites that can interfere with their right to impart and receive information. This can also make it harder for such groups to find web-hosting providers.[17] The Convention on Cybercrime requires States Parties to criminalise such attacks.[18]

Rules regarding discrimination against specific content providers or types by Internet Service Providers are also important for freedom of expression (and innovation). The Committee of Ministers declared in 2010 that: "users' right to access and distribute information online and the development of new tools and services might be adversely affected by non-transparent traffic management, content and services' discrimination or

---

[12] Note 3 p. 20

[13] Yildirim v. Turkey, no. 3111/10, § 31, 18.12.2012

[14] Decision n° 2009-580 § 12, 10.6.2009

[15] Article 5A(2), The Constitution of Greece, as revised by the parliamentary resolution of May 27th 2008 of the VIIIth Revisionary Parliament

[16] Regina v. Smith & Others [2011] EWCA Crim 1772 § 20

[17] Committee of Ministers, Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, § 4, 7.12.2011

[18] ETS 185, § 5, 23.11.2001

impeding connectivity of devices," and suggested that the Council provide guidance to member States or private sector actors on "network neutrality" that would prevent this.[19]

Communications surveillance

The UN Special Rapporteur on freedom of expression issued a prescient report in April 2013 on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression. He identified "an alarming trend towards the extension of surveillance powers beyond territorial borders" and concluded: "Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society."[20]

Revelations from former US National Security Agency contractor Edward Snowden since June 2013 have made clear that the US, UK and allies have built very large scale Internet surveillance systems, with cooperation from Sweden, Denmark and other member States.[21] Twenty-three members of the Parliamentary Assembly have tabled in response a motion for a resolution on "Massive Eavesdropping in Europe", expressing serious concern "about the recent allegations on extensive surveillance and collection of private data by intelligence services".[22] The members recalled the Court's judgment that "States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate" given "the danger such a law poses of undermining or even destroying democracy on the ground of defending it".[23] The Bureau has sent the motion to the Committee on Legal Affairs and Human Rights for the preparation of a new report, to be presented within two years. The motion also "Calls upon the Secretary General to launch an inquiry under Article 52" of the Convention.[24]

Cultural expression and products

Article 10 protects individuals' access to cultural expression and entertainment.[25] To protect creators, innovators and producers of cultural products, the Court has recognised that Article 1 of Protocol No. 1 protects intellectual property rights (such as

[19] Committee of Ministers, Declaration on network neutrality, 29.9.2010

[20] A/HRC/23/40, §§ 64 and 81, 17.4.2013

[21] Caspar Bowden, The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights, European Parliament Civil Liberties Committee, 24.9.2013

[22] Doc. 13288, 6.8.2013

[23] Klass and others v. Germany, no. 5029/71, § 49, 6.9.1978

[24] ECHR § 52: "On receipt of a request from the Secretary General of the Council of Europe any High Contracting Party shall furnish an explanation of the manner in which its internal law ensures the effective implementation of any of the provisions of the Convention."

[25] Khurshid Mustafa and Tarzibachi v. Sweden, no. 23883/06, § 33, 16.12.2008

patents and trademarks), while also stressing that property rights must be balanced against other matters of general interest.[26]

There have been two main Internet-specific challenges in achieving this balancing of rights in Europe. The first is related to the use of trademarks, particularly in the Domain Name System used to translate human-readable addresses (such as hub.coe.int) to numerical addresses. This system is managed by the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit Californian corporation. The Committee of Ministers has recognised "the need to apply fundamental rights safeguards to the management of domain names" and invited Council of Europe bodies to work with ICANN to ensure decisions take full account of international human rights law.

This is particularly important in ICANN's current "new gTLD" programme, under which companies have applied to create thousands of new "global top-level domains", such as ".book". However, civil society groups have criticised some aspects of the management of this programme, with one expert complaining that ICANN has over-privileged protection of trademarks, and that "the real policy process occurred outside of and after the formal policy development process, in chaotic and politicized interactions among the staff, the US government, the [Governmental Advisory Committee] and a trademark lobby that was deliberately targeting ICANN's supervisors in the U.S. government."[27]

Secondly, several member States have introduced powers for expedited sanctions against Internet users accused of (but not held to have) infringed copyright– up to the termination of their Internet service – and procedures for ordering ISPs to block access to sites facilitating copyright infringement. Under the French "HADOPI" law, a court could order the disconnection of a user accused of infringement three times.[28] This provision was recently repealed,[29] following political controversy and doubts that the system was cost-effective. A similar "three-strikes" rule was introduced in a court-approved settlement between right holders and Ireland's largest Internet Service Provider, Eircom, following their application for an injunction imposing such a rule; [30] but other Irish ISPs have refused to introduce this system. The UK's Digital Economy Act 2010 contains provisions requiring ISPs to send warning letters to customers accused of copyright infringements, with right holders able to request from ISPs a list of all customers that have passed a threshold of such warnings in order to bring suit. The government may order ISPs to impose "technical measures" on such customers, including slowing down or terminating their connections. However, none of these measures have yet been brought into force, due to significant political opposition. The

---

[26] Note 3 p. 18

[27] M Mueller, *Meltdown III: How top-down 'implementation' replaced bottom-up policymaking*, Internet Governance Project blog, 14.9.2013. See also the US National Telecommunications & Information Administration web pages on the "IANA Functions Contract" at http://www.ntia.doc.gov/page/iana-functions-purchase-order

[28] *Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet*, 30.10.2009

[29] *Décret n° 2013-596 du 8 juillet 2013 supprimant la peine contraventionnelle complémentaire de suspension de l'accès à un service de communication au public en ligne et relatif aux modalités de transmission des informations prévue à l'article L. 331-21 du code de la propriété intellectuelle*

[30] *EMI Records & Others v. Eircom Ltd* [2010] IEHC 108

UN Special Rapporteur in 2011 stated: "cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, [is] disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights."[31]

Self-regulation and safe harbours

The EU's E-Commerce Directive protects "hosting providers" against liability for storing user files, unless they have "actual knowledge of illegal activity or information" or fail to act "expeditiously to remove" content when they gain such knowledge, encouraging them to act upon notification of copyright infringement by right holders.[32] This has given rise to concern from the UN Special Rapporteur and others that providers may not adequately validate such notices, and are not in a position to carry out a balancing of interests before removing material (including assessing the impact upon their customers' freedom of expression).[33]

The Committee of Ministers has stressed the importance of procedural safeguards for social networking services, "in line with the right to be heard and to review or appeal against decisions, including in appropriate cases the right to a fair trial, within a reasonable time, and starting with the presumption of innocence." It has also recommended that users be provided with "clear information about the editorial policy of the social networking service provider in respect of how it deals with apparently illegal content and what he considers inappropriate content and behaviour on the network."[34] The Committee has also recommended that search engine providers should only discard search results in accordance with Article 10(2) of the Convention; de-indexing or filtering should be "transparent, narrowly tailored and reviewed regularly".[35]

It is relatively easy for courts to order websites within their jurisdiction to remove copyright-infringing materials (or other types of illegal material, such as the almost universally criminalised images of child abuse). Where such materials are hosted outside their jurisdiction, courts have increasingly issued injunctions requiring ISPs to block access to those sites. The High Court of England and Wales, for example, has issued such orders in respect of two sites it found to facilitate large-scale copyright infringement: Newzbin2[36] and The Pirate Bay.[37] In Russia, right holders may obtain an order from the Moscow City Court to have infringing video content removed from a

[31] Note 10 §

[32] § 14, OJ L 178, 17.7.2000, pp. 1–16

[33] Note 10 § 42

[34] Committee of Ministers, *Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services*, §§ 5 and I.3, 4.4.2012

[35] Committee of Ministers, *Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines*, § 8, 4.4.2012

[36] *Twentieth Century Fox Film Corp & Others v. BT plc* [2011] EWHC 1981 (Ch)

[37] *Dramatico Entertainment Ltd & Others v. British Sky Broadcasting Ltd & Others* [2012] EWHC 268 (Ch)

website within three days. Where this does not happen, Russian ISPs may be ordered to block access to this site.[38]

However, the ECtHR has emphasised that a careful weighing of interests must take before blocks are ordered, especially where they impact large sites, since such prior restraint of expression requires the "most careful scrutiny".[39] The Court is considering a claim that over-broad blocking of sites containing infringing musical works infringed Article 10.[40] In two cases, the Court of Justice of the EU has found that requirements for Internet Service Providers or social networking sites to monitor all customer data for infringing works were contrary to EU law for several reasons, including their disproportionate impact on individuals' freedom to receive or impart information under the EU Charter of Fundamental Rights.[41] The Committee of Ministers has declared that general blocking measures should be used only against "clearly identifiable content, […] if the competent national authorities have taken a provisional or final decision on its illegality."[42]

Self-regulatory action by Internet intermediaries such as ISPs and hosting providers, often encouraged by the statutory provision of liability "safe harbours", has advantages in terms of flexibility and the ability to incorporate private-sector expertise and commitment. However, these schemes commonly lack substantive protection for individual rights and due process. Unlike the US Digital Millennium Copyright Act § 512, the E-Commerce Directive does not even contain a provision for users to contest a copyright infringement notice. UK ISPs voluntarily block access to web pages or sites determined by an industry-funded body, the Internet Watch Foundation (IWF), to contain criminal images of child abuse, but only some of them notify users that try to access a blocked page (in other cases presenting a generic error page). Nor does the IWF automatically notify blocked sites; their appeal procedure has been used only once, unsuccessfully, when a Wikipedia page was blocked. This scheme was developed in the face of heavy informal government pressure and threats to legislate.[43]

More recently, the UK government has put pressure on broadband ISPs to ask all customers about blocking access to a much wider range of content, with some options enabled by default, to protect children. Categories under discussion include pornography, weapons and violence, extremism, terrorism, file-sharing, gambling, anorexia, eating disorders, suicide and self-harm, alcohol, smoking, "esoteric" material, and web blocking circumvention tools. Some of these are already blocked by default by mobile ISPs; customers must explicitly request access and show they are adults.[44] "Web-

---

[38] Federal Law of the Russian Federation No. 187-FZ. See also legal analysis by ARTICLE 19 at http://www.article19.org/data/files/medialibrary/37202/Russia's-new-legislation-on-online-copyright-enforcement-.pdf

[39] Note 13 § 47

[40] *Akdeniz v. Turkey*, no. 20877/10

[41] *Scarlet v. SABAM*, Case C-70/10, 24.11.2011; *SABAM v. Netlog*, Case C-360/10, 16.2.2012

[42] Note 9

[43] I Brown, Internet self-regulation and fundamental rights, *Index on Censorship* 1 pp. 98-106, 2010

[44] J Killock, *Sleepwalking into censorship*, Open Rights Group blog, 25.7.2013

blocking circumvention tools" include systems (such as Virtual Private Networks) that the German privacy commissioners (and many others) have recommended that individuals use to protect their privacy online.[45]

Hate speech and incitement to violence

There is a significant challenge in fighting online hate speech and incitement to violence against individuals or groups – while recognising that freedom of expression includes speech that may "offend, shock or disturb".[46] Hate speech is not protected by Article 10 of the Convention.[47] States have a wider margin of appreciation when taking measures against remarks that incite violence,[48] and there is a "category of clearly established historical facts – such as the Holocaust – whose negation or revision would be removed from the protection of Article 10 by Article 17".[49] While criminal measures may be most appropriate for the "most egregious" hate speech, other types may be better met with "educational, cultural, informational and other non-regulatory" measures.[50]

Authors of online hate speech have a high degree of mobility, and can publish material on American sites that have the broad constitutional protection of the US's First Amendment. This means that blocks or bans targeted at specific websites are not effective remedies. Web hosting companies, including social networking sites, have different contractual provisions regarding hate speech; many are reluctant to act as private censors. Different levels of liability potentially attach to different types of Internet companies, depending on their level of editorial involvement and other contextual factors; "a multiplicity of different actors could be involved in the creation and dissemination of hateful content: creating or sourcing it; publishing it; developing it; hosting it or otherwise facilitating its dissemination, accessibility or retrievability."[51]

Twenty States have ratified the Council's Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[52] Prosecutors of authors must strike a careful balance to provide deterrence without chilling free expression. Over-broad laws can be

---

[45] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, *Keine Umfassende Und Anlasslose Überwachung Durch Nachrichtendienste! Zeit Für Konsequenzen*, 5.9.2013

[46] Note 4

[47] *Gündüz v. Turkey*, no. 35071/97, § 41, ECHR 2003-XI

[48] *Sürek v. Turkey (no. 1)* [GC] (no. 26682/95, § 62, ECHR 1999-IV)

[49] *Lehideux and Isorni v. France*, 23.9.1998, § 47, Reports of Judgments and Decisions 1998-VII. Article 17: "Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention."

[50] T McGonagal, *The Council of Europe against online hate speech: Conundrums and challenges*, Background paper for Polish Government and Council of Europe conference "The hate factor in political speech – Where do responsibilities lie?" Warsaw, 18-19.9.2013, pp. 4-6, 28-29

[51] *Ibid*.

[52] ETS 189, 28.1.2003

abused to stifle criticism.[53] England and Wales' Crown Prosecution Service has recently published guidance on prosecuting cases involving communications sent via social media.[54]

Two relevant recent cases relate to a new Russian law prohibiting "promotion of non-traditional sexual relations among minors,"[55] and anti-Semitic content on social media site Twitter. The Russian law provisions have been criticised by civil society groups as vague, subjective, and without any scientific evidence demonstrating a connection with the health and education of children.[56] This will make it potentially risky for civil society groups to counter homophobic speech in Russia. The law imposes an administrative fine more than ten times higher when such information is disseminated by the media and/or information and telecommunication networks.

In 2012 the *Union des Étudiants Juifs de France* (UEJF) successfully asked Twitter to suspend some of the accounts responsible a flood of tweets with the tags "#unbonjuif" and "#unjuifmort". UEJF won a court order requiring Twitter to provide details of the users behind those accounts to the French authorities. In 2012 Twitter introduced a policy allowing tweets to be withheld from specific jurisdictions following receipt of what the company believes to be a "valid and applicable" legal request, which was used for the first time in relation to the account of a German neo-Nazi group. Twitter will attempt to notify the author of withheld content, and users that attempt to access it.[57]

Other matters

A significant challenge to online freedom of expression comes when member States take measures that are not justified under the Convention. Recent examples include cases in Azerbaijan, where bloggers have been jailed for expressing their views and three European intergovernmental organisations have suggested the need for stronger judicial review of cases.[58] A civil society coalition has strongly criticised new laws extending criminal defamation and insult to online content.[59] Freedom House has also criticised recent Russian laws that recriminalize defamation and expand website blacklisting, including political sites occasionally caught under a "vague definition of extremism", with bloggers facing "questionable criminal prosecutions" and regional

[53] Note 50 pp. 27-29

[54] http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/

[55] Federal Law of June 29, 2013 No. 135-FZ "On Amendments to Article 5 of the Federal Law On Protection of Children from Information Harmful to their Health and Development"

[56] *Russia: Federal laws introducing ban of propaganda of non-traditional sexual relationships*, ARTICLE 19, June 2013

[57] Twitter, Tweets still must flow, *The Twitter Blog*, 26.1.2012

[58] *Joint statement on media freedom by European Commission, Council of Europe and Organisation for Security and Cooperation in Europe*, 9.11.2012.

[59] International Partnership Group for Azerbaijan, *New legislative amendments further erode rights to freedom of expression and peaceful assembly*, 16.5.2013

courts ordering "blocking of websites that unveil local corruption or challenge local authorities."[60]

Freedom of the media

The media's role as a "public watchdog" makes its right to impart and receive information under Article 10 particularly important, especially where it contributes to discussions of legitimate public interest.[61] Justifications for limitations on public access to such information must be particularly compelling.[62] The Court has commented: "In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally."[63]

The Committee of Ministers has declared that people increasingly depend upon online media "to access and exchange information, publish content, interact, communicate and associate with each other", fulfilling a role as a social "watchdog".[64] In particular, search engines "enable a worldwide public to seek, receive and impart information and ideas and other content in particular to acquire knowledge, engage in debate and participate in democratic processes",[65] while social media "promote the exercise and enjoyment of human rights" and "offer great possibilities for enhancing the potential for the participation of individuals in political, social and cultural life."[66]

State regulatory frameworks must ensure effective protection of journalists' online freedom of expression.[67] The Court has found: "having regard to the important role the Internet plays in the context of professional media activities and its importance for the exercise of freedom of expression…the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press".[68]

Attacks on and the jailing of journalists are a serious problem in Europe, and have also occurred against online media and bloggers. The Council of Europe, OSCE and European Commission have called for the release from detention of "of all those journalists, bloggers and citizens reporting, who have been deprived of their liberty as a result of expressing their views" in Azerbaijan.[69] In other recent cases, a Slovenian blogger was

---

[60] *Freedom on the Net 2012: A Global Assessment of Internet and Digital Media*, 24.9.2012, p. 13

[61] *Observer and Guardian v. the United Kingdom*, Series A no. 216, § 59, 26.11.1991

[62] *Timpul Info-Magazin and Anghel v. Moldova*, no. 42864/05, 27.11.2007

[63] *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, nos. 3002/03 and 23676/03, § 27, 10.3.2009

[64] Note 17 § 2

[65] Note 35, § 1

[66] Note 34, §§ 1-2

[67] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, no. 33014/05, 5.5.2011

[68] Note 67 § 64

[69] Note 58

jailed for six months for defamation and insults,[70] while a website editor was attacked and beaten by assailants in Bosnia-Herzegovina two days after the first screening of her documentary on the 1991-1995 war.[71]

Protection of sources and whistle blowers

The protection of sources and whistle blowers are vital for online as well as traditional media. The Parliamentary Assembly has affirmed that "the protection of journalists' sources of information is a basic condition for both the full exercise of journalistic work and the right of the public to be informed on matters of public concern"; that anyone should be able to submit information confidentially to journalists; and that "Internet service providers and telecommunication companies should not be obliged to disclose information which may lead to the identification of journalists' sources in violation of Article 10 of the Convention."[72]

This importance of this issue has been highlighted by Edward Snowden's revelations of the large-scale Internet surveillance activities of US and UK intelligence agencies. If this government surveillance of a substantial part of all Internet communications (and collection of "metadata" about them) continues, it will be much more difficult for journalists to protect their sources, particularly those revealing controversial or potentially illegal government activities. The editor of the *Guardian* newspaper, which published many of Snowden's exposés, told an interviewer: "The ability of reporters to report securely is intensely threatened by the collection of metadata,"[73] while MIT Media Lab expert Ethan Zuckerman has said: "I am terrified for journalists because its very hard to promise anonymity to sources."[74]

The Parliamentary Assembly's Committee on Legal Affairs and Human Rights has adopted a report on national security and access to information, which highlights the importance of "the protection of bona fide disclosures of wrongdoings".[75] It endorses the view of experts that "legitimate national security interests are, in practice, best protected when the public is well informed about the State's activities, including those undertaken to protect national security."[76] Twenty members of the Parliamentary Assembly have supported a motion for a recommendation for an additional protocol to the Convention on the protection of whistle blowers who disclose governmental action violating international law and fundamental rights.[77]

---

[70] Reporters Without Borders, *Blogger gets six months in jail for defamation*, 16.5.2013

[71] Reporters Without Borders, *Website editor attacked and beaten over documentary*, 23.7.2012

[72] Recommendation 1950 (2011)

[73] @JeffJarvis, 20.9.2013, at https://twitter.com/jeffjarvis/status/380838240913461248

[74] @TowCenter, 20.9.2013, at https://twitter.com/TowCenter/status/380837947891007488

[75] Doc. 13293, 3.9.2013

[76] *Global Principles on National Security and the Right to Information*, 12.6.2013, drafted by 17 NGOs and five academic centres

[77] Doc. 13278, 5.7.2013

This situation has been further aggravated by the demand of the UK government that the Guardian newspaper destroy the computer in their London offices holding materials from Edward Snowden, and the arrest of Guardian journalist Glenn Greenwald's partner David Miranda as he transited through the country.[78] One Parliamentary Assembly member has asked the Committee of Ministers: "The British authorities have put pressure on the newspaper *the Guardian* to hand over the files which Edward Snowden has given to the newspaper. In addition, the authorities have detained David Miranda at Heathrow Airport for several hours… Does the Committee of Ministers find the behaviour of the British authorities in the two cases consistent with the United Kingdom's commitments to secure media freedom? Does the Committee of Ministers agree that anti-terrorism legislation should not violate fundamental freedoms as media freedom and freedom of expression?"[79] The ECtHR has found that: "the right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources, but is part and parcel of the right to information, to be treated with the utmost caution." Investigating authorities must properly balance "the public interest in the protection of the journalist's freedom of expression, including source protection and protection against the handover of the research material."[80]

Defamation

Information published by the media can have a significant negative effect on individuals' reputations. This is dealt with by defamation laws in most States in cases of "pressing social need" – but without a careful balancing of rights, these laws can damage freedom of expression and the media, especially where journalists are threatened with imprisonment. The Parliamentary Assembly has resolved that member States should abolish jail sentences for defamation "without further delay," and that States should set a maximum period within which libel actions can be brought, outside exceptional circumstances.[81] This is important for online media archives, which are explicitly protected by Article 10, although journalists have an even greater duty to verify the accuracy of published information when there is no urgency.[82]

Freedom of expression and the media can be limited to protect individual privacy, even where information has already been published online. However, the media need not pre-notify individuals before publishing information about them.[83]

---

[78] A Rusbridger, David Miranda, schedule 7 and the danger that all reporters now face, *The Guardian*, 19.8.2013

[79] Written question No. 643 to the Committee of Ministers, Doc. 13298, 9.9.2013

[80] *Nagla v. Latvia*, no. 73469/10, §§ 97 and 101, 16.7.2013

[81] Resolution 1577 and Recommendation 1814 of the Parliamentary Assembly, *Towards decriminalisation of defamation*, 2007

[82] Note 63

[83] *Mosley v. the United Kingdom*, no. 48009/08, 10.5.2011

Media diversity and literacy

One of the most significant issues raised by the Internet is its impact on media diversity and pluralism. It enables many more individual, institutional and media voices to be heard through low-cost and advertising-supported platforms (such as ISP-hosted personal websites, blogging platforms, microblogs, and other types of social media). Search engines facilitate access to information, but can present challenges to human rights through "from the design of algorithms, de-indexing and/or partial treatment or biased results, market concentration and lack of transparency about both the selection process and ranking of results."[84] New Internet services have also contributed to large reductions in the revenue streams that traditionally supported newspapers and their journalists, and to a lesser extent radio and television services. This has "weakened the ability of the press to act as an effective agent of public accountability by undermining the economic basis of professional reporting and fragmenting the public. If we take seriously the idea that an independent press serves an essential democratic function, its institutional distress may weaken democracy itself."[85]

The ability of all persons to participate in this online media environment, regardless of background, is key to maximising the individual and social benefits of the Internet. Programmes to develop digital literacy can encourage civic participation, support informed decision-making and reduce risk from harmful content to young people (such as violence and self-harm, pornography, discrimination and racism) and behaviours (such as grooming, bullying, harassment or stalking).[86] The Conference of Ministers responsible for Media and New Communication Services resolved that media literacy "is a particularly important tool in optimising children's and young people's comprehension, critical thinking, citizenship, creativity and critical awareness".[87] The Committee of Ministers has recommended the promotion of literacy regarding search engines, "in particular on the processes of selecting, ranking and prioritising of search results", and the existence of search alternatives.[88]

Freedom of assembly and association

Article 11 of the Convention protects peoples' right to meet, protest, and organise. Marches, pickets and processions have played a central part in modern European political history, bringing together large numbers of people to protest in pursuit of a collective goal and attract wider attention through the media[89] – which can all be

[84] § 4

[85] Note 1 p. 235

[86] Committee of Ministers, *Recommendation Rec (2006)12 on empowering children in the new information and communications environment*, 27.9.2006

[87] 1st Council of Europe Conference of Ministers Responsible for Media and New Communication Services, *A new motion of media?* 29.5.2009, MCM(2009)011

[88] § 8

[89] DJ Harris, M O'Boyle, EP Bates and CM Buckley, *Law of the European Convention on Human Rights, 2nd edition*, 2009, Oxford University Press, p. 516

facilitated by the Internet. Trades unions (explicitly protected in Article 11(1)) and other social/political organisations have both protected and enhanced individual rights, and formed the core of social movements that overturned totalitarian regimes across eastern Europe, ending the Cold War.

Most social movements now take full advantage of online tools to recruit and organise members. Article 11's protection extends to non-political associations, such as those "protecting cultural or spiritual heritage, pursuing various socio-economic aims, proclaiming or teaching religion, seeking an ethnic identity, or asserting a minority consciousness" – and even, applying a test developed after the European Commission on Human Rights explicitly considered the question, the right of intelligence agency staff to join a trade union.[90] Interferences are tested against a similarly strict standard of review to Article 10.[91]

The main themes of cases before the Court have been "tolerance of peaceful dissent, pluralism in opinion, with some allowance for disturbance to others, and the lawfulness of government interference."[92] Alongside freedom of expression, the Committee of Ministers has declared that: "The right to freedom of assembly and association is equally essential for people's participation in the public debate and their exercise of democratic citizenship, and it must be guaranteed in full respect of Article 11 of the Convention… (without any online/offline distinction)." [93] The Committee has particularly emphasised the potential of social networking services to "facilitate democracy and social cohesion", and recommended these companies "ensure accessibility to their services to people with disabilities, thereby enhancing their integration and full participation in society."[94]

Interferences with online freedom of expression (and privacy) often have an impact on freedom of assembly and association, but much less has been decided or written on the latter as distinct from the former.[95] The emphasis in the latter is on the role and implications of new communication technologies as tools for political debate, participation (including participation of vulnerable and disadvantaged persons), protest and other forms of expressions of discontent.

Freedom of association protects the right of individuals to form groups to protect their interests – including political parties, even those that "call into question the way a State

---

[90] *Ibid*. p. 547

[91] *Ibid*. p. 531

[92] *Ibid*. p. 547

[93] Note 17 § 1

[94] Note 34 §§ 2 and 6

[95] See *Palomo Sanchez and others v. Spain* (Application Nos. 28955/06, 28957/06, 28959/06 and 28964/06)) for an analysis of the relationship between Articles 10 and 11 in a trade union dispute. For an interesting discussion of the right of online assembly in the US Constitution, see JD Inazu, Virtual Assembly, *Cornell Law Review 98,* 2012, pp. 1093-1142. Former US Secretary of State Hillary Rodham Clinton stated in her 2010 "Remarks on Internet Freedom" that "The freedom to connect is like the freedom of assembly, only in cyberspace."

See http://www.state.gov/secretary/rm/2010/01/135519.htm

is currently organised, provided they do not harm democracy itself."[96] The Committee of Ministers has declared that "impediments to interactions of specific interest communities should be measured against international standards on the right to freedom of assembly and association".[97] Blocking access to associations' websites, and communications tools such as webmail and social networking sites, can have a significant negative impact on assembly and association. UN Special Rapporteur Frank La Rue has highlighted the danger of "just-in-time" blocking at "key political moments, such as elections, times of social unrest, or anniversaries of politically or historically significant events."[98]

The Turkish authorities' response to nationwide protests since May 2013 illustrates some of these issues. Istanbul prosecutors are investigating protestors that have allegedly insulted the Prime Minister or other officials on Twitter or Facebook, while the government has proposed measures (so far rejected by both companies) to require user information to be provided to investigators.[99] Turkey has previously blocked large sites used by many civil society groups, such as YouTube and Google Sites, with the ECtHR finding such "wholesale blocking of access" was not allowed by Turkish law.[100]

Azerbaijan has been widely criticised by intergovernmental organisations and civil society for extending criminal defamation and insult offences to online expression and public demonstrations in the run-up to the October 2013 elections. Bloggers and activists on social networks have been arrested and sentenced to administrative detention, with campaign groups noting: "constraints on political activism and a lack of media diversity have [previously] made the Internet the main refuge of freedom of expression and political dissent in Azerbaijan."[101]

Online assemblies on private properties

A key challenge for States in protecting Internet freedoms is that so much of the infrastructure supporting online activity is privately owned. How should governments' positive obligation to protect association and assembly on private social media sites be balanced against those sites' private property rights under Article 1 Protocol 1 of the Convention? So far the Court has been very reluctant to protect equivalent physical assemblies, such groups distributing leaflets and collecting signatures in private shopping centres. It has found that Article 10, and by implication Article 11, confers no "freedom of forum," and that changing modes of social interaction do not require "the automatic creation of rights of entry to private property" – although accepting this might arise in a situation such as "a corporate town where the entire municipality is

[96] *Socialist Party v Turkey*, § 47, 1998-III; 27 EHRR 51

[97] Note 17 § 6

[98] Note 10 § 30

[99] S Fraser, Turkey Investigates Social Media Postings That Allegedly Insult Officials, *The Huffington Post*, 27.6.2013

[100] Note 39 § 62

[101] Note 59

controlled by a private body".[102] It is interesting to speculate how far a single social networking service's market share would have to rise to meet this condition.

Communications surveillance and social network analysis

The former UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, noted that:

> *The rights to freedom of association and assembly are also threatened by the use of surveillance. These freedoms often require private meetings and communications to allow people to organize in the face of Governments or other powerful actors. Expanded surveillance powers have sometimes led to a "function creep", when police or intelligence agencies have labelled other groups as terrorists in order to allow the use of surveillance powers which were given only for the fight against terrorism. In the United States, environmental and other peaceful protestors were placed on terrorist watch lists by the Maryland State Police before political conventions in New York and Denver. In the United Kingdom, surveillance cameras are commonly used for political protests and images kept in a database. A recent poll in the United Kingdom found that one third of individuals were disinclined to participate in protests because of concern about their privacy.*[103]

Edward Snowden's leaks have revealed that the US National Security Agency is conducting massive social network analysis of citizens using electronic records about their communications and other activities, creating "sophisticated graphs" of individuals' "social connections that can identify their associates, their locations at certain times, [and] their traveling companions". The NSA is receiving 20 billion "record events" each day, which includes social network site data, 700 million phone call records and 1.1 billion mobile phone records.[104]

If European States (likely the UK, and possibly Sweden and France) are conducting similar data collection and analysis, the proportionality of such interference would be key to its permissibility under Article 11. The UN special rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, has noted (following a visit to the UK) that: "The practice of surveillance and intelligence databases undeniably has a chilling effect on protestors who fear to hold further protests".[105] The Court has ruled that refusal to register an association is a "radical measure", while permanent dissolution of a political party is "drastic", both justified only in exceptional circumstances. However, restrictions on foreign funding have not been prohibited.[106] Where the recording and analysis of all electronic associations and assemblies (and physical proxies, such as mobile phone locations) sits on this spectrum is not yet clear.

---

[102] Note 89 pp. 518-519

[103] A/HRC/13/37 § 36

[104] J Risen and L Poitras, NSA Gathers Data on Social Connections of US Citizens, *The New York Times*, 28.9.2013

[105] A/HRC/23/39/Add.1, 29.5.2013

[106] Note 89 p. 534

Are Distributed Denial of Service Attacks protected as online protests?

Another as-yet speculative question is whether online Distributed Denial of Service attacks, carried out by protestors to block the availability of certain websites, should be protected in the same way as sit-ins or demonstrations on government or private property. The Cybercrime Convention requires such attacks to be criminalised.[107] An example is the attacks on the websites of Visa and Mastercard by the Anonymous online collective when those payment associations blocked donations to WikiLeaks.[108]

Even if the Court accepted this analogy, Article 11 also requires States to keep rival protestors apart, and allows a broad margin of appreciation in restricting an assembly that intentionally causes disruption to activities. The Court will more closely examine the necessity of bans where a peaceful assembly concerns the expression of opinions on a question of public interest, but independently criminal conduct is unlikely to be protected against prosecutions and conviction – even if it is done with the purpose of drawing attention to the cause.[109]

Elements for responses

The Council of Europe's Internet Governance strategy 2012-2015 action plan notes: "Freedom of expression and information regardless of frontiers is an overarching requirement because it acts as a catalyst for the exercise of other rights."[110] As discussed in the previous section, online freedom of assembly and association is closely intertwined with freedom of expression. The first part of this section discusses priority areas for State responses to protect these rights, where Court action may be otherwise difficult or take many years.

The strategy also highlights the importance of multi-stakeholder governance for protecting the Internet's universality, openness and innovation, and the interests of users.[111] The second part of this section discusses the engagement of business, civil society, academia, and the technical community in achieving this aim. This raises more difficult questions about the responsibilities of private actors in protecting human rights.

The EU is undertaking important work in both of these areas. As it accedes to the Human Rights Convention, there should be even greater scope for EU involvement in the Council of Europe's activities.

---

[107] Note 18

[108] E Addley and J Halliday, WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback', *The Guardian*, 9.12.2010

[109] Note 89 pp. 517/21/24

[110] CM(2011)175 final, § 3, 15.3.2012

[111] *Ibid*. § 4

State responses and lines of action

The Council of Europe Committee of Ministers and Parliamentary Assembly have passed a number of declarations, resolutions and recommendations important for protecting online freedom of expression, assembly and association, as already discussed.

In making further progress, the first major challenge for the Council is to agree the best way to encourage the provision of Internet access to all Europeans. This is being considered by the PACE Committee on Culture, Science, Education and Media, as well as the Committee of Experts on Rights of Internet Users. The EU included a universal service obligation in its 2009 electronic communications framework.[112] There have already been suggestions the Council should consider framing Internet access as a human right.[113] This would create a very significant resource and regulatory commitment for the member States, even if much of the investment to build new infrastructure came from the private sector.

The second challenge is to decide how far guarantees should be provided to Internet users of network neutrality, or non-discriminatory access to content and services. The Council organised a two-day multi-stakeholder dialogue on these questions in May 2013, and has participated in the creation of a "dynamic coalition" at the UN Internet Governance Forum to address the details of neutrality guarantees, which are important for network management and security. The European Commission proposed in September 2013 new network neutrality rules,[114] although these have been criticised by civil society as "a corporate power-grab [that] would relegate the rest of citizens and new-entrant innovators to a slower Internet with disastrous effects for freedom and innovation online".[115] The Council of Europe could play an important role in broadening this debate, and in helping to resolve the tensions between promoting human rights while encouraging the private-sector investment necessary for universal access.

In the online environment, the Council's existing work on the decriminalisation of defamation has become even more important, because independent bloggers and activists are even more vulnerable to State action to chill their freedom of expression than those with institutional support.

Wider issues concerning defamation and the protection of reputation need further consideration. The broad availability of online content has led some courts to assert very wide jurisdiction – with London in particular becoming notorious for libel actions where the claimant, defendant, and publication were all outside the UK.[116] In response, the UK's Defamation Act 2013 § 9 introduced new limits on jurisdiction, and could be considered in further research by the Council as one model for dealing with the broad

---

[112] OJ L 337, 18.12.2009

[113] A Mellakauls, *Access to the Internet – a human right?* CDMSI(2012)Misc3Rev

[114] European Commission, *Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent*, COM(2013) 627 final, 11.9.2013

[115] European Digital Rights, Net Neutrality Threatened By The Commission's Draft Regulation, *EDRi-gram* 11.17, 11.9.2013

[116] English PEN and Index on Censorship, *Free Speech is Not For Sale: The Impact of English Libel Law on Freedom of Expression*, 2009

(and difficult) jurisdictional issues raised by the Internet for the protection of human rights. There is otherwise a serious risk of overlapping jurisdictional claims reducing the cross-border availability of material that is legal under international law, but prohibited under culturally specific national rules on subjects such as obscenity.[117] The Committee of Ministers has already noted States' "responsibility to ensure that their actions within their jurisdictions do not illegitimately interfere with access to content outside their territorial boundaries or negatively impact the transboundary flow of Internet traffic," and recommended that States "should co-operate in good faith with each other and with relevant stakeholders at all stages of development and implementation of Internet-related public policies to avoid any adverse transboundary impact on access to and use of the Internet."[118]

A specific issue raised by the popularity of commenting features on media websites is the liability of online publishers for content created by their users. The Court is currently considering a case where damages were awarded against an Estonian news portal for offensive comments made by a reader.[119] The UK again has introduced a new defence for website operators regarding statements by third parties on the site, even where comments are moderated.[120] This type of measure could be further explored as a way to prevent the imposition of intermediary liability damaging the potential of Internet platforms to support third-party speech, identified as a serious problem by UN Special Rapporteur Frank La Rue.[121]

Protecting online cultural diversity and individual access to cultural expression and products in a way that is compatible with freedom of expression and the rule of law remains an area needing further consideration by the Council. An international group of experts convened by the civil society group ARTICLE 19 has developed a set of principles on freedom of expression and copyright, building on international law, which could provide a starting point. They specifically recommend no user disconnection from Internet access on copyright grounds, strict limits on filtering and blocking, and minimisation of intermediary liability, along with a number of other broader principles.[122]

With regard to protecting freedom of expression through the Internet's Domain Name System, one option is that Council of Europe representatives look to play a stronger role at meetings of the Internet Corporation for Assigned Names and Numbers, which manages this system. They could do this by participating in ICANN's existing structures; by coordinating the human rights-related positions of member States within ICANN's

---

[117] D Korff and I Brown, Social media and human rights, *Human rights and a changing media landscape*, Strasbourg: Council of Europe Publications, 2011, pp. 175-206

[118] Committee of Ministers, *Recommendation CM/Rec(2011)8 on the protection and promotion of the universality, integrity and openness of the Internet*, 21.9.2011

[119] *Delfi AS v. Estonia*, no. 64569/09, communicated on 11.2.2011

[120] Defamation Act 2013 (c.26) § 5

[121] Note 10 §§ 38-48

[122] *The Right to Share: Principles on Freedom of Expression and Copyright in the Digital Age*, ARTICLE 19, 2013

Governmental Advisory Council; or even by asking ICANN to consider new mechanisms for receiving advice on international law from the regional human rights bodies.[123]

Dealing with the serious human rights issues raised by the large-scale Internet surveillance revealed by Edward Snowden will take coordinated action by all of the Council of Europe's constituent bodies. The Parliamentary Assembly's Legal Affairs Committee is now considering the motion for a resolution on Massive Eavesdropping in Europe requesting the "Secretary General to launch an inquiry under Article 52 of the European Convention on Human Rights".[124] While this takes place, the Court,[125] Commissioner for Human Rights and Committee of Ministers will have the opportunity to consider the difficult questions raised by these revelations. What substantive limits on State intelligence gathering are needed to meaningfully protect freedom of expression, assembly and association (as well as privacy) in the Internet era? When almost every human activity leaves some kind of digital trace, are effective oversight and procedural rules (alongside specific rules, such as protection for sources and whistle blowers) enough to adequately protect human rights?

Other difficult questions are raised for freedom of expression, assembly and association by State national security and counter-terrorism programmes. The international law principles described by UN Special Rapporteur Frank La Rue are a useful starting point for consideration. He suggested for example that rules banning support for terrorist activities and organisations should only be used to justify restricting expression that is intended and likely to incite imminent violence, and never should apply to political debate, elections, reporting on human rights/government activities/corruption in government, peaceful demonstrations/political activities, and expression of opinion, dissent, religion or belief, including by minorities and other vulnerable groups.[126]

The Committee of Ministers should consider recommending further procedural and substantive standards for "safe harbours" and other self and co-regulatory mechanisms (building on their Recommendations on filters, social networking and search engines), and to legal procedures that allow courts to order blocking – ensuring the impact on freedom of expression, assembly and association are fully taken into account. These could build on the Court's procedural standards deriving from Articles 6 (the right to a fair trial) and 13 (the right to an effective remedy), and the limits the Court has placed on interferences with the rights in Articles 8, 10 and 11, which must:

- Be based on legal rules that are clear, accessible and foreseeable (and to the extent possible are set out in statute law);
- Meet a "pressing social need";

[123] One expert has suggested reconstituting the GAC as a multi-government-stakeholder body, which includes a range of governmental and intergovernmental agencies, as well as minority political party representatives (in the same manner as the CoE Parliamentary Assembly). See: M Mueller, Reform ICANN's Governmental Advisory Committee: Multi-stakeholderize it! *Internet Governance Project* blog, 8.8.2012

[124] Note 22

[125] The author has provided an expert witness statement for an application by Big Brother Watch, Open Rights Group, English PEN and Dr Constance Kurtze against the United Kingdom, Application No: 58170/13

[126] Note 117

- Not be disproportionate to the purpose, nor ineffective;
- Have an "effective remedy", preferably judicial, if they do not meet these tests.[127]

Where a body is given delegated authority to apply such rules, it should be given limited discretion, give reasoned rulings, and be subject to judicial supervision. Blocked sites should be notified and given the opportunity to appeal decisions in full judicial proceedings.[128]

The Committee of Ministers also needs to seriously consider the compatibility with the rule of law of informal State pressure on intermediaries to impose "default" filters on Internet users, which would block access to large quantities of legal expression. Frank La Rue noted in 2011 that insufficiently targeted blocking measures that render a wide range of content inaccessible beyond that which has been deemed illegal are by definition unnecessary or disproportionate.[129]

On hate speech, a recent expert paper for a Council of Europe and Polish government event noted that "the range of harms to be prevented or minimised is varied and complex," and that regulatory action against "egregious" hate speech should be complemented by educational, cultural and informational measures. It recommended the following steps:

- Repurpose the Committee of Ministers' Recommendations (97) 20 and 21 for optimal application in the online environment;
- Foreground online hate speech in the Council of Europe's standard-setting work;
- Provide guidance on the calibration of rights, duties and responsibilities in the digital age, in particular regarding online hate speech;
- Enhance capacity-building and awareness-raising;
- Crowd-source and collaborate in the search for solutions;
- Develop and effectively promote an 'Anti-Hate Speech Pledge' for politicians and political parties.[130]

Supporting the continued vitality and diversity of the news media in the online environment is one of the most difficult challenges facing the Council. The most appropriate responses from different stakeholders will depend on the paths taken as the news media continues to evolve. Specific rules regarding media plurality may have to be further developed.[131] New forms of competition enforcement could help.[132] Educational programmes and other ways of developing new media literacy in children

---

[127] *Ibid*.

[128] *Ibid*.

[129] *Ibid*.

[130] Note 50 p. 35

[131] This discussion goes back at least 15 years at the Council of Europe. See C Marsden, *Pluralism in the multi-channel market: suggestions for regulatory scrutiny*, MM-S-PL(1999)012 § 5.1

[132] I Brown and CT Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age*, Cambridge, MA: MIT Press, 2013

and adults are important.[133] Paul Starr has noted one advantage of the European post-war tradition: "it is hard to see how philanthropy can match the resources that are being lost… Countries with long-established public-service broadcasters may be better equipped, ideologically and institutionally, to deal with the challenges of the media crisis."[134]

Engaging the business sector and other key stakeholders

The businesses and technical communities that run and develop much of the Internet's infrastructure, as well as the civil society groups and academics that campaign for user rights and study online behaviour, are vital stakeholders in protecting Internet freedom. The Committee of Ministers has declared that: "free speech online is challenged in new ways and may fall victim to action taken by privately owned Internet platforms and online service providers. It is therefore necessary to affirm the role of these actors as facilitators of the exercise of the right to freedom of expression and the right to freedom of assembly and association."[135] Former US Secretary of State Hillary Rodham Clinton spoke of the private sector's "shared responsibility to help safeguard free expression. And when their business dealings threaten to undermine this freedom, they need to consider what's right, not simply what's a quick profit."[136]

UN Special Rapporteur Frank La Rue has written that Internet companies have duties to protect users' rights.[137] Korff and Brown summarised these duties: "intermediaries should restrict these rights only after judicial intervention; be transparent to the user involved, and where applicable, to the wider public about measures taken; if possible forewarn users before taking restrictive measures; and minimise the impact of restrictions strictly to the content involved. Finally, there must be effective remedies for affected users, including appeal through procedures provided by the intermediary and by a competent judicial authority."[138]

In June 2011 the UN Human Rights Council unanimously endorsed the Guiding Principles on Business and Human Rights.[139] These set out duties for business to avoid infringing rights and address adverse impacts of their behaviour, as well as to cooperate in remedying such breaches. The principles are being further developed by a UN working group, while the European Commission recently supported the development of specific guidance for the ICT sector. This guidance sets out a process by which companies can undertake human rights due diligence in markets where they operate, analysing the potential impact of company activities on different stakeholder groups.

---

[133] S Livingstone, T Papaioannou, M Mar Grandío Pérez and C Wijnen, Critical insights in European media literacy research and policy, *Media Studies 3*(6) pp. 1-13, 2012

[134] Note 1

[135] Note 17 § 5

[136] Note 95

[137] Note 10

[138] Note 117

[139] A/HRC/17/31, 21.3.2011

The guidance suggests six core elements of a corporate "responsibility to respect" human rights, shown in Figure 1.[140]

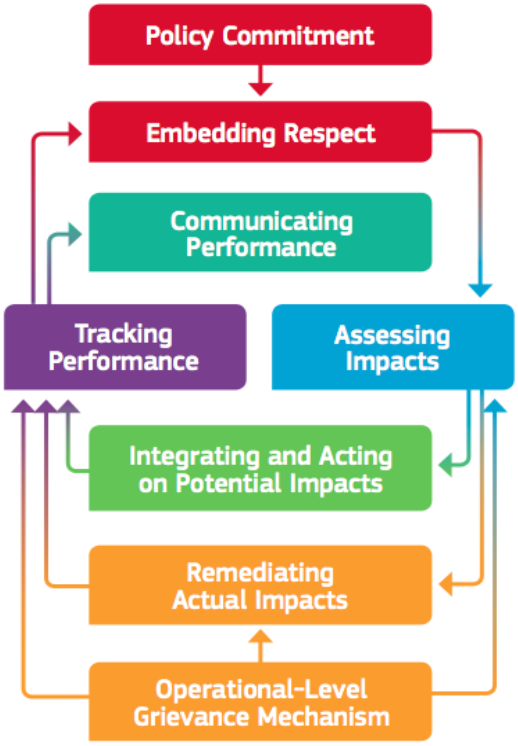

Figure 1: Key Elements of Corporate Responsibility to Respect. Source: European Commission

The Global Network Initiative (GNI) is an example of a multi-stakeholder initiative where technology companies, socially responsible investors, civil society groups and academic experts have developed principles to protect human rights that already go beyond the UN Guiding Principles. States and other stakeholders need to consider further Incentives for engagement in such self-regulatory programmes for key industries (such as telecommunications companies) that so far have played a very limited role. The US Congress has been debating a Global Online Freedom Act that would require Internet companies operating in countries designated as the Secretary of State as "Internet-restricting" to publish details of their policies addressing human rights due diligence. Companies that are members of the GNI or similar initiatives would be exempt from some of the Act's requirements.[141] The Committee of Ministers could consider recommending similar measures.

One element of the UN Guiding Principles already being developed by the Council of Europe is increased transparency by stakeholders in matters such as the number of orders for content to be taken down, or for user data to be supplied to public authorities, and the procedures that are followed to do so. Companies such as Google, Microsoft, Yahoo! and more recently Facebook have published regular statistics on the number and source of such requests. While they were previously barred by US law from doing so for national security-related requests, they are now taking legal action asserting a First Amendment right to do so,[142] and following the Snowden revelations have published summary statistics with the agreement of the US government. Several bills

[140] Shift and the Institute for Human Rights and Business, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, European Commission, 2012

[141] I Brown, The Global Online Freedom Act, *Georgetown Journal of International Affairs 14* (1), 2013, pp. 153-160

[142] Microsoft Corporation, *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, US Foreign Intelligence Surveillance Court Case No. MISC. 13-04, and similar motions by LinkedIn Corporation, Facebook, Inc., Yahoo! Inc. and Google Inc.

before the US Congress would protect this right.[143] The Council of Europe's ongoing multistakeholder process to develop transparency guidelines and commitments could make an important contribution to global transparency.

Acknowledgments

Many thanks to Gabrielle Guillemin, Douwe Korff and Chris Marsden for their suggestions and comments on drafts of this report.

[143] See for example S. 1452 (the Surveillance Transparency Act of 2013) and H.R. 3035 (the Surveillance Order Reporting Act of 2013)