COMMISSIONER FOR HUMAN RIGHTS

COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, February 2012

CommDH (2012)8
Original version

SOCIAL MEDIA AND HUMAN RIGHTS

Issue Discussion Paper

This Issue Discussion Paper was commissioned and published by the Commissioner for Human Rights, to contribute to debate and reflection on media freedoms in Europe. All opinions in this paper do not necessarily reflect the Commissioner's position.

This Issue Discussion Paper is available on the Commissioner's website:
www.commissioner.coe.int

Acknowledgements
This Issue Discussion Paper was prepared by Douwe Korff, Professor of International Law, London Metropolitan University and Ian Brown, Senior Research Fellow, Oxford Internet Institute, University of Oxford.

Table of contents

FOREWORD

Social media come with potential problems, as well as gains. This new phenomenon presents us with a range of fresh challenges. One important issue is how to ensure that Internet regulations do not strangle freedom of expression.

“Blocking”, for example, is nowadays frequently used to prevent specific content from reaching a final user. However, the indications are that this method is not efficient in preventing, for example, human rights violations on the Internet. Furthermore, who should decide what is to be blocked, and what processes and remedies should this be subject to?

The 2011 Report of the UN Special Rapporteur on Freedom of Opinion and Expression is a strong statement of the importance of freedom of expression on the Internet. The Rapporteur emphasises the need for clear rules, in contrast with the arbitrariness he observes today, which allows for increasing surveillance and monitoring of communications.

Restrictions and regulations must be in accordance with Council of Europe standards, and in particular the ECHR and the case law of the Strasbourg Court concerning the narrow set of restrictions to freedom of expression necessary in a democratic society. Also, any interference with the rights to communicate, express views or assemble must be based on rules that are clear, specific and accessible.

Given the crucial importance of these freedoms, such rules should to a large extent be written in statute law, which cannot be easily or quickly changed. To further prevent arbitrariness, any authority to which the power to apply the laws is delegated should be entirely independent, be required to give accessible, transparent and reasoned rulings, and be subject to judicial supervision.

Special attention should be paid to the concept of “incitement to violence”, which should be interpreted in full and effective compliance with the standards in the ECHR and the case law of the Court.

The report from the UN Special Rapporteur, for example, states that, on the important issue of the censorship of alleged support for terrorism, restrictions on the right to expression can only be justified if the government can demonstrate that the expression is intended to incite imminent violence, and that there is a direct and immediate connection between this expression and the likelihood or occurrence of such violence.

In this Issue Discussion Paper Douwe Korff, Professor of International Law at London Metropolitan University, and Ian Brown, Senior Research Fellow at University of Oxford discuss the range of fresh challenges that social media presents us with. They argue that while there is a need to ensure better protection of personal integrity in social media, the right to freedom of expression must not be undermined.

Social networks indeed host a vast and growing repository of personal data, all of it in digital form. It falls to our national and international authorities to ensure that our individual rights to privacy and data protection are not sacrificed to social networks, but rather reinforced to recognise and meet the range of new challenges these powerful new media present.

The principal positions my Office has tried to promote in this area are the following:

- Internet freedom is important. All restrictions must be based on clear, specific and accessible statute law. Those regulatory authorities applying the laws restricting freedom of expression must be entirely independent, accountable and with adequate safeguards in place to avoid arbitrariness;

- Greater transparency and proportionality of Internet blocking is required, including narrowing the grounds for restriction of prohibited content to those accepted by the case law of the Court, and publishing public lists of blocked sites;

- Blocking must be carried out with effective notice on the conclusion of due process, and interested parties should be given the opportunity to challenge the decision in public judicial proceedings.

- There is a need to pursue the discussion about how to ensure protection of individual integrity (data protection) in the social media – without underling the right to freedom of expression.

Thomas Hammarberg

SUMMARY

This Issue Discussion Paper focuses on the human rights issues raised by the use of online social media for political activism. Blogs, video and social networking sites have become a key forum for political debate and organisation – so much so that they have provoked counter-responses from some repressive states.

Section one of this paper describes these counter-measures. Some states have adopted Internet blocking, filtering or takedown procedures or Internet surveillance (including compulsory data retention), or even shut down national networks, in attempts to restrain users' freedoms. And in many otherwise democratic countries, the use of measures such as blocking and monitoring still leaves much to be desired in terms of human rights.

Section two examines the legal issues raised by such counter-measures, and suggests how human rights protections could be improved. We describe the body of principles that aims to orient legislation in Council of Europe member states. Its sources include the European Convention on Human Rights (ECHR) and associated case law – developed primarily for the offline world; other conventions and resolutions, including the Council of Europe Convention on Cybercrime; and an emerging body of Internet governance principles.

Our conclusions indicate three areas that require solutions: a weakness in the European Court of Human Rights' doctrine of discretion for individual states; the need to bolster the role of private sector intermediaries with requirements for them to defend their users' Internet freedoms; and the demands of the rule of law. We propose solutions as a basis for further discussion of what are undoubtedly serious challenges.

Introduction

The Internet and social media have become increasingly important in political activity. Blogging, video-sharing and tweeting were crucial in the political events in North Africa and the Middle East in 2011. They are important to human rights defenders everywhere. But the use of these new technologies to assert old freedoms has been met with repression by some governments.

A recent study of 37 countries by Freedom House cites increasing website blocking and filtering, content manipulation, attacks on and imprisonment of bloggers, punishment of ordinary users, cyber attacks and coercion of website owners to remove content, in attempts by authoritarian states to reduce political opposition. It suggests that Internet restrictions around the globe are partly a response to the exploding popularity, and significant role in political and social activism, of sites like Facebook, YouTube and Twitter. Governments consistently or temporarily closed down such sites in 12 of the countries studied, including Egypt and Tunisia where democracy advocates relied heavily on Facebook to mobilise supporters and organise mass rallies.[1]

Of the various means of suppressing communication by Internet, the most extreme have involved simply cutting off all Internet access (Egypt, January 2011, and Syria at the time of writing),[2] or even creating a completely state-controlled mini-Net (apparently planned by Iran).[3] In other cases, such as Bahrain, governments have used their control over local Internet structure to deliberately slow down connection speeds, in particular at newspaper offices, hotels and homes. Thailand, Burma, China and Iran have tried to manipulate online discussions through organised pro-state submissions. China has pressured search engines to distort search results. In several countries, bloggers and Internet activists have been subjected to threats and physical attack. Following riots in several British cities, the government proposed taking powers to shut down social networking sites during future recurrences. This last proposal was withdrawn after widespread public criticism (but approval from official Chinese media).

Of the eight Council of Europe member states covered by the Freedom House study, four were ranked “Free” in terms of Internet freedom – Estonia, Germany, Italy and the United Kingdom (though this did not mean there were no issues), and four – Azerbaijan, Georgia, Russia and Turkey – were ranked “Partially Free”, meaning they have significant Internet freedom problems.

An interactive “Internet in Europe” map produced by the media innovation group OWNI reveals serious issues throughout the European region, including the four countries ranked “Free” by Freedom House.[4] In 7 of the 24 European countries on which information was available – Belgium, France, Italy, Romania, Spain, Denmark and Sweden – OWNI judged Internet filtering to be “rampant and problematic: (no judge involved in the process, lack of transparency concerning who [that is, what] is targeted, etc.)”.

[1] Kelly S. and Cook S. (eds) (2011), Freedom on the Net 2011: A global assessment of Internet and digital media, Freedom House, Washington, DC; see: www.freedomhouse. org/uploads/fotn/2011/FOTN2011.pdf.
[2] “Syrian Internet shutdown”, Renesys blog, 3 June 2011, see: www.renesys.com/ blog/2011/06/syrian-internet-shutdown.shtml.
[3] “Iran vows to unplug Internet”, Wall Street Journal Online, 28 May 2011, quotes Iran’s head of economic affairs as saying the aim is to create “a genuinely halal network, aimed at Muslims on an ethical and moral level”, largely detached from the worldwide web: http://online.wsj.com/article/SB10001424052748704889404576277391449002016.html.
[4] The map rates countries in six categories: intellectual property (enforcement of protected content); data retention (transposition of the EC Data Retention Directive); mobile (denial of certain functionalities); filtering (including blocking of child pornography and online gambling sites); support for ACTA (the Anti-Counterfeiting Trade Agreement); and copyright (level of piracy). We use the ranking for filtering (though the map only looks at non-political filtering), because the main issue here is one of process rather than of what is being filtered. The maps for filtering and data retention are at: http://owni.fr/2011/05/25/ carte-internet-europe-regulation-filtrage-copyright-droit-liberte-utilisateurs.

I. Measures that states use to interfere with Internet freedoms, and their limitations

1.1 Blocking

Freedom of expression, the free flow of information, and freedom and pluralism of the media have internationally been acknowledged as human rights in the post-Second World War intergovernmental instruments: the Universal Declaration of Human Rights (UDHR, 1948) and the International Covenant on Civil and Political Rights (ICCPR, 1966). In both the UDHR and the ICCPR, Article 19 makes this commitment.

The main aim of blocking is to prevent specific Internet content from reaching a final user, by software or hardware that reviews communications and decides on the basis of pre-set criteria whether to prevent receipt. It does not affect the target material. A common aim is blocking images of child abuse; however, this does not obliterate the images, nor remove them from the Internet. A more effective response would be to remove images from the Internet, criminally investigate producers and save children from such situations. Blocking does none of that.[5] In human rights law, this problem relates to the legal criterion of whether it is effective, and thus "proportional".

Blocking is a broad term: not all types are equally effective, nor legally equivalent. The term may suggest that Internet blocking is easy – like throwing a switch – but the capabilities of the technologies are complex and can often be easily bypassed.[6] Blocking is also subject to "false positives" (blocking of sites with no prohibited material) and "false negatives" (when sites with prohibited material slip through a filter).[7] All blocking technologies reviewed in an Open Society Institute study were flawed in terms of over- or under-blocking. Most were easy to circumvent; all could be circumvented without much effort by determined people.[8] This is good news for political activists in repressive countries, but bad news for states, officials and private entities hoping to use blocking to stop dissemination of child abuse images or hate speech.[9]

In all the countries studied, Freedom House found arbitrariness and opacity surrounding decisions to block content: "in most non-democratic settings there is little government effort to inform the public what content is censored and why." The authorities often avoid confirming that a website has been blocked and instead remain silent or cite technical problems: "even in more transparent, democratic environments, censorship decisions are often made by private entities and without public discussion, and appeals processes may be onerous, little known, or non-existent".[10]

---

[5] Callanan C. et al. (2009), "Internet blocking: balancing cybercrime responses in democratic societies", Aconite/OSI, full report and summary at: www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf; www.aconite.com/sites/default/files/Internet_Blocking_and_Democracy_Exec_Summary.pdf. Blocking activities of selected states have been extensively analysed by others, including one of the authors. See for instance, Brown I. (2008), "Internet filtering – be careful what you ask for", Kirca S. and Hanson L. (eds) Freedom and prejudice: Approaches to media and culture, Bahcesehir University Press, Istanbul.

[6] Chapter 5 of the report summarises the complex range of technology issues, and a brief discussion of the various approaches (target-based, decision-maker-based, etc.) is in the Executive Summary, and Brown (2008), ibid.

[7] For examples of "over-blocking" and its causes see Brown (2008), ibid – including Pennsylvania's Internet filtering law, struck down in 2004 partially because of over-blocking: the blocking of 400 sites had prevented access to over 1.1 million others, while being easily circumvented. The Court found no evidence that the Act "reduced child exploitation or abuse" (CDT v. Pappert, 2004).

8 An overview of evasion technologies (proxy servers, "tunnelling", "hosting or URL rotation", botnets, evading DNS-based filters) is on pp. 18-19 of the Executive Summary of Callanan et al. (2009), op. cit. (note 5) – with a useful chart (p. 17) indicating the characteristics of the various blocking strategies discussed: the likelihood of over- and under-blocking; the resources and maintenance effort required for each; and the intrusiveness in terms of deep-packet inspection (DPI) requirements.

[9] See: Clayton R., "Failures in a hybrid content blocking system", Proceedings of the 5th Workshop on Privacy Enhancing Technologies, Dubrovnik, May 2005, available at: www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf.

[10] Kelly and Cook (2011), op. cit. (note 1), pp. 4-5.

Thus, no one knows what is on the blocking lists of "partially free" Azerbaijan, Georgia, Russia or Turkey. In these and other European countries, the criteria for blocking are totally unclear. The application of blocking is unforeseeable, and effectively unchallengeable.

Once blocking lists are introduced, they can grow. There have been attempts to block sites containing not only hate speech and advocacy of terrorism, but also political debate, information on minority rights, alleged defamation, purported copyright infringement – even the "sacred texts" of Scientology.[11]

1.2 Censorship by pressure

Government officials increasingly contact authors or websites to apply pressure for content to be removed, with threats of legal action, withdrawal of contracts or licences and outright bans – even where companies are based in overseas jurisdictions. A "word in the ear" of a senior executive can be as effective.[12] After all, companies are generally seeking to maximise profit; that is their raison d'être, not the protection of free speech.

Governments also encourage their supporters to complain to hosting companies about user-generated content. YouTube and Facebook have removed or disabled activist accounts in China, Egypt, Ethiopia, Mexico and Tunisia following such complaints.[13]

These pressures raise human rights questions – including the issue of whether companies should have obligations to resist pressure as a means of safeguarding their users' human rights.[14]

1.3 Restrictive measures across country boundaries

Two methods are used to reach across country boundaries to restrict information flow:

The first is direct action (for instance, prosecution) by a state against individuals or companies acting through sites hosted in another state, which has significant implications in human rights law.[15] Examples (discussed in section two) include the conviction by a British court of a French national resident in the United Kingdom (Perrin), who owned and operated a US-based website, and an order by a French court against (US-based) Yahoo! for allowing the offer of items deemed illegal in France to French citizens, on a US-based website.

Secondly, governments may threaten foreign companies, even where the related content is not illegal, with serious commercial sanctions for facilitating dissemination. This raises the question of whether private entities that have the technical responsibility for delivering content should have a legal obligation to defend their users' human rights, even in a foreign context.

1.4 Internet surveillance

The authorities are often interested to know who is trying to access banned material. The famous 1983 Census judgment of the German Constitutional Court said:

> *A social and legal order in which the citizen can no longer know who knows what about him, and when, and in what situation, is incompatible with the right to informational self-determination.*
> *A person who wonders whether unusual behaviour is noted each time, and thereafter always kept on record, used or disseminated, will try not to come to attention in this way …*

[11] Brown (2008), op. cit. (note 5).
[12] Anderson M., "A sneak peek at a fractured web", Wired News, November 13, 2006, at: www.wired.com/news/technology/0,72104-0.html.
[13] Kelly and Cook (2011), op. cit. (note 1), p. 8.
[14] Ibid., pp. 7-8.
[15] In discussing transnational legal action, we exclude actions by states against their own nationals (or residents) for accessing or disseminating material downloaded from other countries – though this may well breach international human rights law (and if in Europe, the ECHR).

> *This would … limit the … common good, because self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens.*[16]

In repressive countries, the purpose of identifying those trying to access banned material may be to target opposition activists. In democracies, such surveillance may easily slip from targeting actual terrorists to those sympathetic to terrorists, or simply those with "extreme" views. For many years, anti-terrorism and emergency legislation has been extended in this way.[17]

The Internet and other modern communication technologies have opened new possibilities for the ubiquitous surveillance of people, on the basis of what they read or discuss, with whom they discuss it, who they "chat" with, what blogs they visit, what online videos they watch or what they upload.

We may think we are free and unobserved when we surf the Internet, chat with friends, send out tweets or upload video clips from our mobile phone. In practice, essentially everything we do or say or watch on the Internet is logged, and in principle available for analy-sis – unless we take elaborate precautions. If we do, that in itself is likely to flag us up to those watching.[18] This allows repressive states to monitor and link activists, with a view to harassment, arrest and worse. Even in liberal democracies, this has led to the monitoring of peaceful activists.

"Simple" surveillance of communication – not capturing content, but monitoring only who communicates with whom, when, where – can be intrusive. This "social network analysis" is increasingly used in investigation and surveillance by police and state security agencies.[19] Repressive countries can easily use it to note, map and target social networks used for political activism.

1.5 Data retention

"Data retention" refers to compulsory retention by communication service providers (including internet service providers, or ISPs) of the communication records of all their clients – beyond the normal (billing) period for keeping data – "just in case" the data might be useful in some future police or secret service enquiry. This ought to be viewed as mass surveillance of citizens without due cause: a fundamental departure from a basic principle of the rule of law.

Under criminal law, repressive measures such as phone secrecy violation, mail opening, searches of premises or people, and arrests are allowed only on the basis of indications that a criminal offence has been committed, and indication of a specific individual's involvement in it. Countries use different terms such as "reasonable suspicion" and "factual indications" but all require at least some basis of indication of illegality before intrusive measures are allowed, and correlate the intrusiveness of the measures to the level of real or factual evidence available, and to various procedural safeguards. For example, when evidence is "soft", relatively unobtrusive measures are typically authorised, with relatively light procedural requirements (in an urgent case, perhaps no more than a requirement for an official record and a post facto review). More intrusive measures (house searches, arrest, etc.) require strong indications of criminal acts and personal involvement, and authorisation by a court.

[16] BVerfGE Bd. 65, S. 1 ff. (our translation).
[17] See, for example, from our own experience: Korff D. (1983), "Aspects of the law regarding freedom of expression in the Federal Republic of Germany", later used (with the author's trial observation report on the case against Haag et al.) in the AI publication "Prosecution for the exercise of the right to freedom of expression in the Federal Republic of Germany", AI Document EUR 23/02/85, London, 1985, or Korff D. (1986), "Criminal-legal restrictions on freedom of expression in Israel and the Occupied Territories", used in an AI Submission to the Israeli Government later that year.
[18] Brown I. and Korff D. (2009), "Terrorism and the proportionality of Internet surveillance", European Journal of Criminology, 6(2), pp. 119-134.
[19] Opening page to: "Revealing links: The power of social network analysis – A new i2 White Paper", Issue 1, May 2010. The rest of the paper provides important further descriptions and illustrations.

Compulsory data retention rides roughshod over this principle. It is an affront to the rule of law, to the very principles that the Council of Europe stand for – and a signal to countries in other parts of the world that such a basic principle can be set aside if deemed inconvenient. This is why it has faced such forceful opposition, and why constitutional and other courts in several European Union (EU) member states have ruled it to be incompatible with fundamental rights.

Even so, the executive and political arms of the EU – the European Commission and the EU Council – have been pressing on with the concept, and are even taking legal enforcement action against several states which have not implemented the EU Data Retention Directive (Directive 2006/24/EC), or which have had to withdraw draft laws implementing it, because they violated the state's national constitution. An evaluation report by the European Commission was rightly dismissed as a "whitewash" by civil liberty and civil society organisations.[20]

As European Digital Rights (EDRi) and other organisations point out, European bodies, including the EU and the Council of Europe, cannot on the one hand object to interference with the rights of online activists in oppressive countries, while on the other hand introduce, and forcefully pursue, the very same kind of measures, with the same absence of control and oversight, against their own populations.

These measures are also in breach of fundamental European human rights – including those in the ECHR and in the Charter of Fundamental Rights of the EU. This is the opinion not only of civil liberty groups, but also of the official EU monitor on this subject, the European Data Protection Supervisor.

II. Applying human rights and emerging Internet governance standards to political activism and counter-measures on the Internet

2.1 Basic legal principles, criteria, interpretation

The interrelated freedoms of communication, expression and asso-ciation are at the heart of any free, democratic society based on the rule of law. From the relevant articles (8, 10, 11) of the ECHR, the Strasbourg Court has developed standard basic tests to be applied to restrictions placed on these rights, which must:

- be based on "law", that is on legal rules that meet quality require-ments of clarity, accessibility and foreseeability;
- serve a legitimate purpose in such a society, that is a "pressing social need";
- be "necessary" to achieve that purpose, that is they must not be disproportionate to the purpose, nor ineffective;
- have an "effective remedy", preferably judicial, if they do not meet these tests.[21]

[20] EDRi, 17 April 2011 at: www.edri.org/data-retention-shadow-report. The text of the Data Retention Directive (full title: Directive 2006/24/EC of the European Parliament and of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) can be found at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. The Commission evaluation report is at: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf; and the full EDRi "shadow evaluation report" is at: www.edri.org/files/shadow_drd_report_110417.pdf.

[21] See: Harris D. et al. (2009), Law of the European Convention on Human Rights, (2nd edn), Chapter 8 (Articles 8-11: General Considerations), Chapter 14 (Article 13: The Right to an Effective Remedy) and Chapter 6 (Article 6: The Right to a Fair Trial). For a simpler overview of these standards, see Korff D., "The standard approach under Articles 8-11 ECHR and Article 2 ECHR", available from: www.coehelp.org/mod/resource/view.php?inpopup=true&id=2130. For details of the application of these principles in the field of freedom of expression, see the Council of Europe Human Rights Handbook on Article 10, available from: www.coehelp.org/file.php/54/ resources/Handbooks/art_10_eng.pdf.

These standards are expressed in the case law of the Court and other international human rights bodies, such as the Human Rights Committee, which applies the provisions of the International Covenant on Civil and Political Rights (ICCPR).

2.2 Application in practice – mitigated by the doctrine of "margin of appreciation"

The Strasbourg Court's famous 1976 Handyside judgment, on the banning of the publication in England of the Little Red Schoolbook on the grounds that it "corrupted public morals",[22] states a firm principle: freedom of expression is one of the essential foundations of a "democratic society", a basic condition for its progress and for every person's development, applicable (subject to Article 10.2), not only to "information" or "ideas" that are regarded favourably, or as inoffensive or with indifference, but also to those that offend, shock or disturb the state or any sector of the population. The judgment noted: "Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society.'"

The Handyside judgment, applying this to "protection of morals", qualifies the powerful dictum under Article 10.2, by saying that, since there is no single European conception of morals visible in each state's law, and since local laws on morals change by time and place, state authorities themselves are better placed than an international judge to give an opinion on the exact content of each country's requirements in terms of morals, and whether any restriction on the freedom of expression is "necessary" to meet "a pressing social need". Consequently, the Court considered that Article 10.2 leaves to contracting states a "margin of appreciation".

However, Article 10.2 does not give contracting states unlimited "appreciation". The Court can give a final ruling on whether a restriction or penalty is reconcilable with freedom of expression as protected by Article 10. The margin of appreciation goes "hand in hand with" European supervision, which applies to the aim of the measure challenged, and its "necessity", as well as to the decision applying it. The judgment refers to Article 50 of the ECHR ("decision or ... measure taken by a legal authority or any other authority"), and its own case law.

Since the Handyside judgment, the margin of appreciation doctrine has been applied to all substantive articles of the ECHR. It has made the Court's case law somewhat unpredictable, but certain factors bear on the scope of the "margin". A degree of European agreement or even harmonisation on an issue narrows that scope. If there is little or no agreement on the substantive issue, and no harmonisation of law, a state might be given a relatively wide margin of appreciation. Because societies are seen as differing substantially on the issue of what is "necessary" to protect "public morals" – they are allowed, for instance, to limit publications in their jurisdiction that are permitted elsewhere.

In practice the Court addresses freedom of expression only peripherally; it asks not whether the state in question struck the right balance between freedom of expression and competing interests, but rather whether the state restricted the right to such an extent that it brought itself outside the broad scope of what was more or less deemed to be acceptable throughout Europe. The only exception is when there are clear European standards in a specific field or when there is clear, strong convergence in European state practice.

For the purpose of this Issue Discussion Paper, it suffices to note that the "margin of appreciation" continues to allow considerable differences in national standards on such things as pornography, incitement to racial hatred, defamation and privacy. As we shall discuss below, this poses serious problems in the new globalised digital environment.

2.3 Procedure and due process: the ECHR and the international approach

The ECHR has two "due process" provisions. It requires:

– in Article 6, that states provide a "fair trial", with many specific guarantees, to anyone whose "civil rights and obligations" are "determined" in some forum, or faces a "criminal charge";

[22] Handyside v. the United Kingdom, Appl. No. 5493/72, judgment of 7 December 1976, paragraph 49.

– in Article 13, that states provide an "effective remedy" to anyone whose ECHR rights and freedoms are violated.

In our opinion, any assessment of the legality and legitimacy of acts of political activism on the Internet ought to be determined in full and fair judicial proceedings fully conforming to the requirements of Article 6, ECHR.[23] That would bring European human rights law in line with the long-established principle expressed by the Supreme Court of the United States of America almost half a century ago that only a judicial determination in an adversary proceeding "suffices to impose a valid final restraint", because it "ensures the necessary sensitivity to freedom of expression".[24]

2.4 The Convention on Cybercrime: weak reaffirmations of the basic principles

The Council of Europe Convention on Cybercrime, with its Additional Protocol, requires state parties to criminalise various activities in cyberspace, including "distributing, or otherwise making available, racist and xenophobic material to the public through a computer system."

However, in our assessment its human rights provisions – covering process and procedure, substantive law, and interpretation – are generally weak, leaving the issues in question almost entirely to the states. In fact, they do little to clarify the ECHR requirements in cyberspace and should be strengthened through guidance and interpretation.

It is positive, however, that the convention contains provisions for the prohibition of indiscriminate surveillance and collection of large amounts of communications data.

2.5 The emerging Principles of Internet Governance

Certain principles stated by the Council of Europe Reykjavik Declaration and the Global Network Initiative (GNI) Principles, especially their emphasis on states' "positive obligations" and the responsibility of information and communication technology (ICT) companies (such as ISPs and search engines), make important contributions to ensuring effective respect for the human rights of online activists (and others). However, they do little to clarify how these high-minded principles should be applied in practice.

Two other documents go further, and spell out at least some further implications in some detail. These are Recommendation CM/Rec(2008)6 of the Council of Europe's Committee of Ministers on measures to promote respect for freedom of expression and information with regard to Internet filters, and the May 2011 Report of Frank La Rue, the UN Special Rapporteur on Freedom of Opinion and Expression, on the promotion and protection of the right to freedom of opinion and expression. Following on from the Rapporteur's previous (2010) report, the latter focuses on trends and challenges to all individuals' right to seek, receive and impart information and ideas of all kinds through the Internet.[25]

We shall discuss them in turn.

[23] Much case law, and academic debate on the Convention, has focused on the definition of "civil rights and obligations" and "criminal charge" – the qualifying factors for "fair trial" under Article 6 (if the issue is outside them, the person can rely only on the "effective remedy" of Article 13). We do not go into this distinction here, because in practice most cases related to political activism clearly fall within Article 6: they result from (criminal) investigation, prosecution, imprisonment or harassment; because the European Court of Human Rights increasingly reads elements of the judicial protection under Article 6 into the requirements of Article 13; and because we see the distinction as anachronistic – drafted in the 1950s when many states' due process in administrative (e.g. tax) law fell short of the "fair trial" requirements. Today, the ICCPR simply says that "everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law" in determining any rights arising in any "suit at law" (criminal or not).

[24] Freedman v. Maryland, 380 U.S. 51 (1965), available from: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=380&invol=51.

[25] Human Rights Council, 17th session, 16 May 2011, A/HRC/17/27: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

2.6 The Reykjavik Declaration

In 2009 the Council of Europe Conference of Ministers responsible for Media and New Communication Services adopted the Reykjavik Declaration. The intention was to stress the need to ensure European human rights standards are upheld on the Internet. Though repeating commitments expressed, in similarly vague terms, in earlier declarations and recommendations,[26] the Reykjavik Declaration also notes the heavy reliance of the Internet on non-state actors (including private sector bodies such as ISPs), and on critical technical resources (such as "root servers" and "backbone structure") "which are controlled by a variety of government authorities, including re-designated defence agencies, academic institutions and private/ business entities."[27]

The Reykjavik Declaration does not explicitly designate access to the Internet as a fundamental right, but comes close by stressing that "the notion of positive obligations developed in the case law of the European Court of Human Rights is particularly relevant in this context."[28] Also, the Committee of Ministers had already concluded in its recommendation on measures to promote the public service value of the Internet that "access to and the capacity and ability to use the Internet should be regarded as indispensable for the full exercise and enjoyment of human rights and fundamental freedoms in the information society.[29]

In other words, even if access to the Internet per se is not a human right, in the modern world all Council of Europe member states have a positive obligation to provide or at least a duty to allow it. Failure to do so, or measures to restrict access, inherently constitute interferences with rights protected under the ECHR, most notably the right to freedom to [seek,] receive and impart information and ideas regardless of frontiers, which is an integral part of the right to freedom of expression (Article 10, ECHR) and the right to respect for [confidentiality of one's] correspondence (an "autonomous concept" that has already been stretched to include all forms of communication) (Article 8, ECHR).[30]

2.7 The GNI Principles

The Principles on Freedom of Expression and Privacy drawn up by the GNI[31] make an important contribution by specifically including private sector entities in these obligations.

They include somewhat basic reaffirmations of the need for compliance on the Internet with international free expression and privacy standards, and even more basic references to the need

[26] See the long list and summaries of such earlier declarations and recommendations on p. 30 of the Background Text, at: www.coe.int/t/dghl/standardsetting/ media-dataprotection/conf-internet-freedom/Internet%20governance_en.pdf.

[27] Political declaration and resolutions from "A new notion of media ?" adopted by the Ministers responsible for Media and New Communication Services from the 1st Council of Europe Conference of Ministers responsible for Media and New Communication Services, held on 28 and 29 May 2009 in Reykjavik, available at: www.coe.int/t/dghl/standardsetting/media/MCM%282009%29011_en_final_web.pdf, in particular the Resolution on Internet governance and critical Internet resources (pp. 9-10) and the Resolution on developments in anti-terrorism legislation in Council of Europe member states and their impact on freedom of expression and information (pp. 11-12). These instruments include Resolution CM/Rec(2007)16, referred to later in the text.

[28] Paragraph 3. See also paragraph 8: "Council of Europe member states share the responsibility to take reasonable measures to ensure the ongoing functioning of the Internet and, in consequence, of the delivery of the public service value to which all persons under their jurisdiction are entitled."

[29] Recommendation CM/Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet, at: https://wcd.coe.int/wcd/ ViewDoc.jsp?id=1207291. See also the Internet Governance Principles, adopted at the COE conference "Internet freedom: From principles to global treaty law", April 2011, available in draft form at: www.coe.int/t/dghl/standardsetting/media-dataprotection/ conf-internet-freedom/Internet%20Governance%20Principles.pdf.

[30] This has been formally re-stated as the right to respect for one's communications in Article 7 of the EU Charter of Fundamental Rights.

[31] GNI, founded in 2009, describes itself as "a diverse coalition of leading information and communications companies, major human rights organizations, academics, investors and technology leaders", who seek to protect and advance freedom of expression and privacy in ICTs. See: www.globalnetworkinitiative.org. This page also has links to the GNI Principles, the Implementation Guidelines for the Principles, and the Governance, Accountability and Learning Framework for the Principles.

for compliance with the rule of law in matters affecting freedom of expression on the Internet. But they add that ICT companies "have the responsibility to respect and protect the freedom of expression and privacy rights of their users" and that "the development of collaborative strategies involving business, industry associations, civil society organizations, investors and academics will be critical to the achievement of these principles." Subscribing companies must "integrate these principles into company decision making and culture through responsible policies, procedures and processes, and a transparent governance structure that supports their purpose and ensures their long-term success."

2.8 More specialised instruments and reports that add clarification and principles

In our opinion the Council of Europe Recommendation CM/ Rec(2008)6 adds important new detail to the basic ECHR principles, in particular on transparency, procedural safeguards and involvement of the private sector. It sets out guidelines on use and application of broadly applied filters (that is, excluding user-controlled filters and those aimed at restricting access by children). These include protection for freedom of expression and privacy; requirements for filtering to be proportionate and only carried out by public bodies for reasons specified in Article 10.2 of the ECHR; and that blocking decisions be reviewable by an independent tribunal.

2.9 Report of the UN Special Rapporteur on Freedom of Opinion and Expression

The 2011 Report of the UN Special Rapporteur on Freedom of Opinion and Expression is a strong statement of the importance of freedom of expression and its exercise on the Internet.

The Rapporteur places great emphasis on the need for proper, judicial procedures in relation to anything that affects the right to Internet freedom of expression, contrasted with the arbitrariness he observes in many respects, including surveillance and monitoring of communications.

In terms of substantive law (what kinds of restriction on Internet free speech are warranted), he supports decriminalisation of defamation, worldwide. And on the important issue of censorship of alleged support for terrorism or terrorist organisations, he emphasises that national security or counter-terrorism measures can only be used to justify restricting the right to expression if the government can demonstrate that the expression is intended to incite imminent violence, is likely to incite such violence, and there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

Quoting Handyside – that the right to freedom of expression includes "views and opinions that offend, shock or disturb" – and stating areas to which restrictions should never be applied (for example political debate; elections; reporting on human rights; government activities; corruption in government; peaceful demonstrations/political activities, including for peace or democracy; and expression of opinion, dissent, religion or belief, including by minorities/vulnerable groups), he emphasises the need for clear and unambiguous laws as a basis for any censorship/blocking/filtering, because broad, ambiguous laws are a basis for arbitrariness. He adds the important supplementary principle that:

> *Any legislation restricting the right to freedom of expression must be applied by a body which is independent of any political, commercial, or other unwarranted influences, in a manner that is neither arbitrary nor discriminatory, and with adequate safeguards against abuse, including the possibility of challenge and remedy against its abusive application.*

The Rapporteur says that blocking lists should not be secret, because "this makes it difficult to assess whether access is being restricted for a legitimate purpose", and that insufficiently targeted blocking measures that render a wide range of content inaccessible beyond that which has been deemed illegal are ipso facto an unnecessary or disproportionate means of achieving the purported aim.

He points out the drawbacks of "notice-and-takedown" measures, as "subject to abuse by both State and private actors", because intermediaries, as private entities, are not best placed to determine whether a particular content is illegal and "censorship measures should never be

delegated to a private entity". He also notes that no one except the author should be held liable for content and that takedown should in principle occur only on a court order, after due process.

The Rapporteur welcomes the GNI, stressing that companies have duties, and that to avoid infringing users' rights to freedom of expression and privacy, 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.

III. Problems in applying the emerging principles

The emerging body of principles indicates, more precisely than the basic principles of the ECHR or the case law under it, how the rights and freedoms (as well as duties and responsibilities) governing Internet political activism can, and cannot, be regulated. They centre on requirements for clearer laws reflecting strict substantive limits on limitations of free speech, applied by accountable bodies, and subject to judicial oversight; on shielding intermediaries from liability, subject to transparent ex post facto takedown procedures, again subject to effective judicial oversight; on imposition of duties on private sector entities (such as those intermediaries) to uphold freedom of expression, even where that conflicts with short-term commercial interests; and on guaranteeing unlimited access to the Internet for all.

We summarise these emerging principles in our conclusions and recommendations, and wholeheartedly endorse them. However, they do not resolve difficult legal issues under the relevant European and international standards, in particular the ECHR, which have been largely ignored or glossed over through vague statements merely reaffirming the need to uphold those standards. We believe this gives rise to a need to resolve three main difficulties in the:

– application of the "margin of appreciation" doctrine by the Strasbourg Court;
– rights and duties of private entities that play a crucial role in maintaining the Internet;
– guarantee of the rule of law and due process in everything related to the Internet.

3.1 The "margin of appreciation"

The doctrine of "the margin of appreciation" has resulted in uneven application of ECHR standards in different countries, even within the Council of Europe.

We believe the jurisdictional issue is central in relation to freedom of expression and communication, and thus to political activism, online. It can no longer be dismissed as a mere "difficulty" (as in the Perrin case, below): it is a core problem.

Under Handyside, courts in a European jurisdiction "A", could, today, order domestic ISPs to block content published from jurisdiction "B" (which could be a European or a non-European country) where its publication is legal, and could convict the author or publisher for breaching the domestic law of "A" (for instance for obscenity, incitement or defamation). The ban or conviction could be in accordance with the ECHR even if there were no ban anywhere else in Europe.

In the Strasbourg Court case with this profile – Perrin v. the United Kingdom[32] – a British court had convicted Perrin, a French national living in the UK, for a publication on a US-based site by a US-registered company he controlled. The UK Court asserted jurisdiction since the website could be accessed from the UK and the material was held to breach UK obscenity laws. However the site complied with its laws of origin (California, US). The issue was whether the material was obscene under Section 2 of the 1959 Obscene Publications Act. Perrin had argued that UK courts

[32] Admissibility Decision of 18 October 2005 in Appl. No. 5446/03, Perrin v. the United Kingdom, accessed through HUDOC. The case is one of a number of cases listed in a May 2011 European Court of Human Rights Factsheet on new technologies, available at: www.echr.coe.int/NR/rdonlyres/CA9986C0-BF79-4E3D-9E36-DCCF1B622B62/0/ FICHES_New_technologies_EN.pdf.

could convict only when the major steps towards publication took place in the UK;[33] the UK Court of Appeal ruled this would undermine the aim of the UK law, by encouraging publishers to take publication steps in countries where they were unlikely to be prosecuted, adding that "there is … difficulty with the worldwide web, but it is through the worldwide web that people are able to make very substantial profits".

Nothing more was said about the "difficulty". Perrin submitted to the Court the argument on "major steps" in the UK being required for UK courts to have jurisdiction, but the Court dismissed it on the basis that as a UK resident, he had reasonable access to UK laws, and as the site was a professional activity, he could reasonably have been expected to be cautious in his occupation – and should have taken legal advice.

The Court referred to Chauvy and Others v. France, in which it had held that, as a professional, an applicant publisher must at least have been familiar with the applicable legislation and case law and could have sought advice from specialist counsel. But this was for a hard-copy, offline publication, in France, by French applicants, with no international aspect.

We feel that in Perrin the Strasbourg Court did not sufficiently address the crucial issue, and accepted applicability of UK law too readily, without sufficiently detailed reasoning. By simply dismissing the jurisdictional point, it missed an opportunity to clarify application of the ECHR to Internet publication. It failed to seriously examine the closeness or otherwise of the link between the applicant, the US company, and the UK, for example in terms of visitors to the website.

In the Yahoo! case, a French court ordered Yahoo! of the US to block access to US-based auctions of Nazi items or content denying the Holocaust. Yahoo! argued that such an order could not apply in the US, as it would violate the US Constitution's First Amendment (guaranteeing freedom of speech to every citizen). But the order was imposed. The case has not been taken to the Strasbourg Court; the US courts have refused to deal with the issues of principle.[34]

In an academic note a decade ago,[35] Tim Fitzpatrick noted that if a German judgment can rule any website accessible from Germany to be subject to German law, websites would be subject to the laws of every country, resulting in an anarchic legal framework fraught with contradictions. The Yahoo! case foreshadowed the challenge of creating a global governance system: that of determining when a foreign court can make a valid, binding ruling over an Internet company. If the process gathered momentum, he said, "the legal infrastructure that the Internet is built upon" would "crumble under the weight of unlimited and unsolvable conflict"; while on the other hand, if countries cannot regulate, many countries' fragile social compromises might be undermined.

The dilemma remains unresolved. Guidance is urgently required. It could come from the Strasbourg Court, intergovernmental guide-lines or a treaty.

In view of the crucial need to preserve the Internet's openness, neutrality and limited regulation (principles strongly supported by the Council of Europe),[36] we feel the Strasbourg Court's current approach is too accommodating to member states and cannot be retained without modification in the context of the Internet; it leads inevitably to those "unlimited and unsolvable conflict[s]".

[33] Here we are not discussing whether the Obscene Publications Act is clear enough to be regarded as "law" in terms of the ECHR, nor whether the applicants' conviction was disproportionate, for example.
[34] See the Case Analysis of the International League Against Racism and Anti-semitism (LICRA), French Union of Jewish Students v. Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000, by Yaman Akdeniz, at: www.cyber-rights.org/ documents/yahoo_ya.pdf. As this case summary notes: "The French approach … is similar to the German approach in which Compuserve was found liable under German criminal law for the distribution of illegal content over the Internet (mainly child pornography). The [German] decision came despite the efforts of the Prosecution who agreed with the defence that 'it was technically impossible to filter out all such material' over the Internet." Local court (Amtsgericht) Munich, English version of the case at: www.cyber-rights.org/isps/somm-dec.htm. See also "[U.S.] Court throws out Yahoo appeal in Nazi memorabilia case", 12 January 2006, by Juan Carlos Perez, at www.infoworld.com/print/20138.
[35] Fitzpatrick T. "Establishing personal jurisdiction in cyberspace: Can anyone govern Yahoo?", UCLA J.L. & Tech. Notes 1, at: www.lawtechjournal.com/notes/2001/ 01_010417_fitzpatrick.php.
[36] See in particular the Council of Europe's draft Internet Governance Principles and CM/Rec(2007)6.

Member states should no longer be given the excessive protection of overgenerous application of the “margin of appreciation” on the Internet.

Solutions are not easy; but neither member states nor the Strasbourg Court should chase chimeras. The pretence that member states can stop the sea of information at their virtual borders by court order is unsustainable.

Ordering intermediaries to filter out search results, or ISPs to block transmission of an e-book, does not prevent access to it by anyone keen to find it; such measures are trivially easy to circumvent – while their imposition signals that states remain free to impose their own divergent restrictions.

3.2 Overcoming Yahoo!

There is an important distinction to be made between material that is unlawful in one country but not in others, and material that is unlawful under international law. In our opinion, in cases where material is legal to produce and disseminate in one country, and illegal in others, the law should be directed at those who download the material. The state that has criminalised this material ought to focus on its own jurisdiction and prosecute those who download. If instead the law is directed at intermediaries, such as ISPs, it will be largely ineffective in tackling both the production and availability of the material and will have a significant detrimental effect on free expression.

We believe Perrin’s conviction could be compatible with the ECHR if it was shown that he had personal primary responsibility for the materials: that the site specifically targeted or clearly attracted UK visitors in significant numbers – and that no measures were in place to dissuade UK visitors from entering the site.

Those who oppose certain content may not be satisfied with our proposal, but should understand that convictions such as Perrin’s and blocking orders like that against Yahoo! are of limited effectiveness in preventing access to the material. We consider such measures to be neither necessary nor proportionate. Also, if Perrin’s conviction was to stop him “corrupting morals”, it may stop him while in prison, but will not prevent seekers finding comparable sites publishing from anywhere, nor imitators.

In the case of material that is unlawful under international law (child abuse images, incitement to racial hatred, etc.), states should take action to prohibit materials, here primarily targeting producers rather than consumers. States should take steps to co-operate in doing so.

For all material that is unlawful in one country, but not others, we suggest it must be established whether a restriction is compatible with substantive European and international standards; then it must be determined whether it obeys the requirement of the UN Special Rapporteur and the UN Human Rights Council, that restrictions should never be applied to political debate, reporting on human rights, government activities or corruption, election campaigns, peaceful demonstrations or political activities, or expression of opinion, dissent, religion or belief.

This would leave states the right to impose restrictions on certain forms of material such as pornography or incitement. But, on these, states should no longer be given wide margins of appreciation as to freedom of expression. They should be allowed to impose measures on their own nationals and residents, for downloading materials that are unlawful under their domestic law (provided that the domestic law complies with the ECHR). But they should not be allowed to penalise companies and individuals in other countries where the materials are lawful (and not contrary to international criminal law), for making the materials available.

3.3 Rights and duties of private sector entities

The ECHR governs action (or inaction) by states, not private entities. States’ duties are mainly “negative”, for example to abstain from torture. But in some cases the Strasbourg Court has

imposed "positive obligations" on states – including to "secure" enjoyment of a right.[37] When it extends these to matters between private parties, this is called the ECHR's "indirect horizontal effect": it has held, for example, that a state has a duty to stop employers from dismissing people who refuse to accept compulsory trade union membership,[38] and to provide sanctions against a man who abused a child with intellectual disability.[39] Impositions causing these indirect effects are rare, and the ruling is against the state, not the private transgressor. It is left to the state to decide how to deal with the private entity – and the state is left a very wide margin of appreciation to choose measures to ensure respect for the relevant right.

We believe that securing rights to communication, expression and association on the Internet, vis-à-vis ISPs, search engines and blog hosts, for instance, should not be left to the very indirect, haphazard application of "horizontal effect".

The emerging Internet governance principles, including the GNI Principles on Freedom of Expression and Privacy, have recognised this. We believe these (or similar) principles should be given greater legal backing as a vital precondition for protection of human rights in the information society.

One way of achieving this would be through the conditioning of the invocability of intermediary (especially ISP) liability exceptions upon compliance with such a self-regulatory initiative. This means that as long as the intermediary (ISP) follows certain rules and procedures (as set out in such initiatives), it will not be liable for any act by its customers alleged to be in breach of criminal or civil law. See, for example, Articles 12 to 15 of the EU E-Commerce Directive,[40] or s.230 of the US Communications Decency Act.[41]

The substantive and procedural rules in question could be endorsed (formally or otherwise) in national or European law. This is a new area, and new, "blue-sky" thinking is needed. However, we note that one alternative, the creation of yet more treaty systems, is not much encouraged these days.

With significant endorsement, such a system of rules might be a major means to ensure good governance, and respect for fundamental rights, on the Internet, especially if it included a reporting and supervisory mechanism (now usual in international human rights treaties). It might gain added force if companies that signed up to it would obtain some benefit (other than goodwill), such as allowing states to give them preferential treatment in the awarding of Internet-related contracts, without being in breach of World Trade Organization rules.

3.4 The rule of law and due process: guaranteeing compliance

We have deliberately emphasised the less difficult, but crucial (and not yet resolved) issue of the rule of law and due process. Our points are in line with similar views of the UN Rapporteur. We recommend that:

- any interference with the freedoms to communicate, express views or organise be based on rules that are clear, specific and accessible. Given these freedoms' crucial importance, such rules should to a very large extent be spelled out in statute law (rather than left to subsidiary rules or ministerial orders, for example, which can be too easily made and quickly changed, and are often insufficiently accessible);

[37] See the requirement in Article 1 of the ECHR that all state parties "shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention."
[38] Young, James and Webster v. the United Kingdom, Appl. Nos. 7601/76, 7806/77, judgment of 18 October 1982.
[39] X and Y v. the Netherlands. Appl. No. 8978/80, judgment of 26 March 1985.
[40] Directive 2000/31/EC of the European Parliament and of the Council, 8 June 2000, on legal aspects of information society services, in particular e-commerce, in the Internal Market ("Directive on electronic commerce"), OJ L 178, 17.7.2000, p. 1-16.
[41] 47 USC para. 230.

- these rules prevent arbitrariness: any authority to which the power to apply them is delegated should not be given excessive discretion, should be required to give reasoned rulings, and should be subject to judicial supervision:
    - substantive restrictions on freedom of expression should obey the limitations on such restrictions spelled out by the UN Special Rapporteur on Freedom of Opinion and Expression and the UN Human Rights Council (as quoted above);

    - any surveillance measures must respect the prohibition (in the Convention on Cybercrime) on "general or indiscriminate surveillance and collection of large amounts of traffic [and communications] data". Compulsory suspicionless retention of such data, currently required under EU law, violates this principle and also, in our view, the ECHR and the EU Charter, as well as several national constitutions;

- any blocking or filtering be based on published lists or criteria, drawn up by properly designated bodies, supervised and accountable under public law or to parliament;

- actual blocking be in principle carried out only after due notice to those involved (both the owners of sites to be blocked and the public), since blocking a site not only prevents the host from publishing, but everyone else from receiving;

- such notice be followed by proper, full, public judicial proceedings (in very urgent cases, a judge should be able to issue temporary injunctions, on the usual restricted basis and subject to equally urgent hearings and challenges);

- legal aid be available to those affected, including civil society groups with an interest in the case, who should be given right of standing, for instance through class actions: individuals and civil society groups should not have to face punitive financial risks for taking such action;

- to the extent that entities of the private sector impose or give effect to restrictions on the above freedoms, they be subject to the above conditions exactly in the same way as entities of the public sector, possibly through the new international rules discussed above, and pending that, by their state of establishment taking responsibility for their actions, and through enforceable "third party beneficiary" clauses in relevant contracts, etc.

IV. Conclusions and recommendations

We have examined the significant human rights issues raised for member states of the Council of Europe by the potential of online social media as a tool of political activism, as recently demonstrated by events in the Middle East and North Africa, and state counter-measures they have provoked: in particular, Internet blocking, takedown procedures and Internet surveillance (including surveillance-facilitating measures such as compulsory data retention).

These measures have become increasingly prevalent in Council of Europe member states due to legitimate state concerns about online criminal activities, particularly online exchange of child abuse images. However, due to the limitations inherent in these restrictive measures, Internet blocking does not serve the aim of removing targeted content from the Internet (and does little, for example, to protect children from abuse). It is highly intrusive; ineffective in preventing determined users from accessing illegal content; inevitably blocks legal content; and can sometimes assist those against whom it is used.

Moreover, it is often based on vague, arbitrary laws (or no law at all); usually relies on secret lists, unknown to the public and drawn up by unaccountable bodies; and is seriously lacking in due process, both when applied as prevention – with exclusion of stakeholders, notification and a right

to object to blocking – and after the fact, in terms of challengeability (would-be publishers and recipients are both unable effectively to challenge lists or decisions).

Far from providing a free, unwatched space for social and political interaction, Internet technologies can facilitate potentially comprehensive surveillance over online political action – increasingly linked to offline surveillance of political activities, in particular through "social network analysis" and "profiling". This is facilitated in a most pernicious way, not only in manifestly repressive countries but also in modern democracies through compulsory suspicionless mass communication data retention under the EU's Data Retention Directive. Such measures have been held to violate fundamental rights and basic principles of the rule of law by national constitutional courts in several EU member states, and by the European Data Protection Supervisor.

The Strasbourg Court has established basic principles relating to the closely linked rights of communication, expression and association. Restrictions on these freedoms must be based on legal rules that meet important "quality" requirements of clarity, accessibility and foreseeability; that serve a "pressing social need"; are "necessary" to achieve that purpose, implying that they shall not be disproportionate or ineffective; and offer an "effective remedy", preferably judicial, against such restrictions.

The Council of Europe's Convention on Cybercrime contains rather basic, and qualified, affirmations of these principles, but also a more useful prohibition against "general or indiscriminate surveillance and collection of large amounts of traffic [and communications] data". Emerging principles of Internet governance reflect a growing consensus on the need for principles governing the activities of private sector entities involved in the maintenance of the Internet, or as intermediaries between the Internet and individual users. There have also recently been important new clarifications and developments of the well-established principles in relation to the Internet, as contained in particular in Council of Europe Committee of Ministers Recommendation CM/Rec(2008)6 and especially the May 2011 Report of the UN Special Rapporteur on Freedom of Opinion and Expression to the UN Human Rights Council.

There are a number of difficulties in applying these new, emerging principles relating to online freedoms of communication, expression and association. We have identified three issues that cause particular problems in this regard.

First, in an age of global communication and information exchanges, states should no longer be given the excessive protection accorded to them by the overgenerous application of the "margin of appreciation" doctrine. We propose a much more restrictive application of the doctrine, to deal with the reality of the Internet, because in our opinion the pretence that states can stop the sea of information at their virtual borders is unsustainable.

Second, we conclude that the ECHR as currently applied is insufficient to regulate the actions of private entities involved in the day-to-day operation of the Internet. It should not be left to the indirect, haphazard application of the doctrine of horizontal effect to secure the rights to communication, expression and association of everyone, including political activists, on the Internet vis-à-vis ISPs, search engines and blog hosts, for example.

In our opinion, the emerging Internet governance principles (which specifically extend to private sector entities) should become legally enforceable. This could be achieved through minor, but crucial, changes to existing rules on intermediary liability.

Finally, we have spelled out in some detail the requirements of the rule of law, as we see them, in relation to political activity on the Internet. These include:

- the need to base all restrictions on clear, specific and accessible rules, in statute law;
- limits on delegated authority and on measures that could lead to arbitrariness;
- transparency over Internet blocking;
- the establishment of due process and ex post facto judicial procedures in respect of blocking, with full involvement of civil society.

The private sector entities that effectively control much of what happens on the Internet must also play a key role in protecting these principles.

We believe that the adoption of the above recommendations would greatly strengthen the legal protection of online political activism, and ensure that the potential of the Internet to support human rights is fully developed.

Freedom of expression on the Internet is a fundamental freedom of our age. Together with Internet privacy, it is vital to our freedoms to communicate and associate, and to collectively determine how our societies should be run.