Speaking of terror

By

David Banisar
Speaking of terror

A survey of the effects of counter-terrorism legislation on freedom of the media in Europe
by David Banisar

Media and Information Society Division
Directorate General of Human Rights and Legal Affairs
Council of Europe

November 2008
The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe.

David Banisar is Director of the Freedom of Information Project of Privacy International in London. He is also a Non-Resident Fellow at the Center for Internet and Society at Stanford Law School and a Visiting Research Fellow at the School of Law, University of Leeds. Previously he was a Research Fellow at the Kennedy School of Government at Harvard University and a co-founder and Policy Director of the Electronic Privacy Information Center in Washington, DC. He has also served as an advisor and consultant to numerous organisations including the UN Development Programme, Representative on Freedom of the Media for the Organization for Security and Co-operation in Europe, the Organization for Economic Cooperation and Development, Justice Canada, the Open Society Institute, Article XIX and Consumers International. He has worked in the field of information policy for seventeen years and is the author of books, studies, and articles on freedom of information, freedom of expression, media policy, whistleblowing, communications security, and privacy.
Contents

Executive summary, page 3

I. Introduction, page 5

II. Effects of international bodies on Council of Europe member states, page 7
United Nations, page 7
The Council of Europe, page 8
The European Union, page 10

III. Limits on access and gathering information, page 13
Access to Information Laws, page 13
State Secrets Legislation, page 15
Limits on Photography, page 17

IV. Limits on freedom of expression, page 19

V. Protection of journalists' sources and materials, page 25

VI. Wiretapping and surveillance of journalists, page 29

VII. Conclusion, page 35

VIII. Appendix, page 37
Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis, page 37
Declaration on freedom of expression and information in the media in the context of the fight against terrorism, page 40
Executive summary

The effects of anti-terrorism legislation and efforts since 2001 has raised new challenges for the media’s ability to collect and disseminate information. Nearly all European nations have adopted new laws in that period.

The role of international bodies including the Council of Europe (CoE) and the European Union (EU) has been more negative than positive with the adoption of many international agreements that either ignore or only pay scant attention to fundamental human rights and the importance of a free media. The role of European institutions such as the EU and the CoE have resulted in greater adoption and harmonisation of these laws than most other regions.

Freedom of expression has been especially challenged by the adoption of new laws on prohibiting speech that is considered “extremist” or supporting of terrorism. These new laws in many jurisdictions are used to suppress political and controversial speech. Web sites are often taken down or blocked.

Access to information laws have been widely accepted and adopted across the CoE. However, state secret and national security laws are regularly being used against journalists and their sources. There are also growing, mostly unregulated, limits on photography.

Protection of journalists’ sources is also widely recognised both in national laws and in decisions of the European Court of Human Rights (ECtHR). However, these protections are often undermined by governments seeking to identify officials who provide information. Newsrooms are often searched.

New anti-terrorism laws are giving authorities wide powers to conduct surveillance. Sources protections and journalists rights are often undermined by the use of these laws. Other new laws are making it easier to conduct surveillance by imposing technical and administrative requirements on keeping information.
I. Introduction

Since 2001, nearly all European countries have revised their legislation and policies relating to fighting terrorism. New laws have been adopted; old laws have been revised; policies and practices have been changed. Most of these revisions have expended the powers of governments to fight terrorism and other crime. Controls on these powers are often insufficient.

This is not a European only phenomenon and problem. Nations around the globe have adopted anti-terrorism legislation in response to the attacks. This report will focus on some of the changes that affect the ability of the media to collect and disseminate information. The issues reviewed will be examined through the lens of two important instruments on media freedom issued by the Council of Europe (CoE) Committee of Ministers:

In 2005 the Committee of Ministers of the Council of Europe issued a “Declaration on freedom of expression and information in the media in the context of the fight against terrorism”. The Declaration called on member states to respect media rights and to not unnecessarily introduce new restrictions on freedom of expression and information; to not treat journalists’ reporting of terrorism as supporting of it; to ensure access to information, scenes of acts, and judicial proceedings; to protect their sources; and not to pressure them.

In 2007 the Ministers issued further guidelines on “protecting freedom of expression in times of crisis”, including terrorist attacks. The guidelines remind governments of their obligations to ensure that journalists have access to information; that sources and information gathered should not be revealed or seized; that public access to information should not be limited; and that “vague terms” such as incitement should not be used to limit freedom of expression and should be clearly defined.

These two instruments set out a baseline that CoE member states should be following. It is the finding of this study that those guidelines have not been respected by all nations. Journalists have been increasingly placed under pressure in many jurisdictions with detentions, shutting down of newspapers, and prosecutions.

New laws designed to protection national security from terrorism and other threats limit journalists’ ability to access information. There have also been increased procedural powers to obtain information through surveillance, searches, demands for disclosure and other means. At the same time, the laws are used to prosecute journalists for obtaining information from sources and justify surveillance to identify the sources so that journalists can be prosecuted under secrets acts for violating their duties to keep information secret.

Too often, these are used for political rather than public safety reasons. As UN Secretary General Kofi Annan said in 2003, “we are seeing an increasing use of what I call the ‘T-word’ – terrorism – to demonise political opponents, to throttle freedom of speech and the press, and to delegitimise legitimate political grievances.”

Information for this report was gathered from a variety of public sources including reviewing of available laws and case-law, government reports submitted to the Council of Europe Committee of Experts on Terrorism (CODEXTER), the United Nations (UN) Counter-Terrorism Committee (CTC), the UN Human Rights Committee, the Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe (OSCE), and the European Union, as well as reports and analyses produced by the above intergovernmental organisations, along with materials from academics, human rights groups, media organisations and other organisations. This is only a brief snapshot of current trends and thus, it is to be expected that there are gaps in the document based on a lack of available information.

1. Declaration on freedom of expression and information in the media in the context of the fight against terrorism, adopted by the Committee of Ministers on 2 March 2005 at the 917th meeting of the Ministers’ Deputies.
2. Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis, adopted by the Committee of Ministers on 26 September 2007 at the 1005th meeting of the Ministers’ Deputies.
Future work could enhance and clarify the situation by conducting detailed country surveys or audits which focus on the issues covered by the study.

Thanks to Yaman Akdeniz, Heather Brooke, Gus Hosein, and Peter Noorlander for their comments and the many journalists, academics and others who provided information.
II. Effects of international bodies on Council of Europe member states

The initiatives of international bodies in developing international instruments relating to terrorism has been a significant driver in the adoption of anti-terrorism laws in CoE member states. Often, these efforts require that states adopt far ranging laws to fight terrorism while paying little attention to human rights concerns. In some areas, such as surveillance and extremism speech, many member states have gone further than the legal requirements and adopted national legislation which seriously challenges human rights.

This section reviews some of the key instruments that have been adopted by the United Nations, Council of Europe and European Union that affect freedom of expression and freedom of information.

United Nations

The resolutions and the implementation committee of the Security Council have been long criticised by human rights groups, academics, state governments and even UN officials for focusing on adopting legislation and paying little or no attention to the human rights effects of the legislation, ignoring obvious human rights concerns and failing to raise the issue with member states.4

Specific concerns have been raised over freedom of expression. In December 2001 17 Special Rapporteurs from the UN Human Rights Commission including those on free expression, torture, protection of children, and migrants issued a statement expressing concern about the effects of the terrorism laws on the media and other groups:

We express our deep concern over the adoption or contemplation of anti-terrorist and national security legislation and other measures that may infringe upon the enjoyment for all of human rights and fundamental freedoms. We deplore human rights violations and measures that have particularly targeted groups such as human rights defenders, migrants, asylum-seekers and refugees, religious and ethnic minorities, political activists and the media.5

The United Nations was the first international body to propose new measures following the attacks in September 2001. On 28 September 2001 the United Nations Security Council adopted Security Council Resolution 1373.6 The resolution calls on member nations to take measures to fight terrorism including adopting laws on financing or support and sharing information. Article 5 declares that “knowingly […] inciting terrorist acts are also contrary to the purposes and principles of the United Nations.” A committee was set up to promote and evaluate each nation’s efforts.

In September 2005, following the London bombings, the Security Council issued a non-binding resolution proposed by UK Prime Minister Tony Blair which expanded the restrictions on speech.7 The resolution condemns incitement and repudiates justification or

---


However, some observers have noted that it is troubling to have an mechanism on a non-binding resolution. See Bianchi, “Security Council’s Anti-terror Resolutions and their Implementation by member states”, Journal of International Criminal Justice 4 (2006), 1044-1073.
glorification (apologia). It calls on states to adopt measures to “prohibit by law incitement to commit a terrorist act or acts,” “prevent such conduct” and “deny safe haven” to those believed to have done so. It also calls for states to improve border controls and take measures to counter incitement and “prevent subversion of educational, cultural and religious institutions.” In response to some of the previous criticisms, the resolution notes that the measures must comply with states’ obligations under international law, “in particular international human rights law” and refers to Article 19 of the UN Declaration on Human Rights in the recitations.

More recently, the UN has been paying more attention to the subject by issuing additional resolutions on human rights and terrorism and creating a special Special Rapporteur on the Promotion and Protection of Human Rights While Countering Terrorism. The Human Rights Commission adopted resolutions in 2004 and 2005 voiced concerns about the use of counter-terrorism laws to limit free expression. The Commission called on nations to “refrain from using counter-terrorism as a pretext to restrict the right to freedom of opinion and expression in ways which are contrary to their obligations under international law”.


These efforts have increased the recognition of protection of human rights in the context of the fight against terrorism. However, many observers still remain concerned that an imbalance remains with the human rights protections limited to mostly general or declaratory statements while legal obligations which affect human rights are more specifically set out.

The Council of Europe

The Council of Europe has adopted numerous conventions, resolutions and documents on terrorism and related matters over the years. This includes two declarations on protecting freedom of information and freedom of expression in the fight on terrorism mentioned in the first section, and a recommendation on the use of surveillance techniques in anti-terrorism.

An important aspect of all of its work is the necessity for conventions to be compatible with the European Convention on Human Rights (ECHR) and its strong protections of freedom of expression and other human rights.


Following the September 2001 attacks, the CoE created a working group to review its anti-terrorism legislation and began work on the convention in 2003. It opened the instrument for signature in May 2005 and it entered into force in June 2007. The Convention has now been signed by 28 countries and ratified by 15.

The scope of the convention is relatively narrow, focusing mostly on new crimes for public provocation, recruitment and providing training for terrorism. There are also sections on providing assistance for victims.

The Convention goes further than other anti-terrorism treaties and bans not just incitement but also “public provocation” when it “causes a danger” that a terrorism incident “may be committed”. Article 5 on Public provocation to commit a terrorist offence states:

1. For the purposes of this Convention, “public provocation to commit a terrorist offence” means the distribution,

---

8. See e.g. UN, Commission on Human Rights Resolution: 2004/42 The right to freedom of opinion and expression, Human Rights Resolution 2005/38
9. General Assembly resolution 60/288 of 20 September 2006 on “Global Counter-Terrorism Strategy”.
11. See Council of Europe, Committee of Experts on Terrorism, http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/
12. Declaration on freedom of expression and information in the media in the context of the fight against terrorism (2005); Guidelines on protecting freedom of expression and information in times of crisis (2008).
13. Recommendation Rec (2005) 10 of the Committee of Ministers to member states on “special investigation techniques” in relation to serious crimes including acts of terrorism.
14. For an extensive overview, see Council of Europe, Freedom of Expression in Europe: Case-law concerning Article 10 of the European Convention on Human Rights, Human rights files, No. 18, 2007. See e.g. Jersild v. Denmark, App 15890/89; Gerger v. Turkey, App 24919/94; Ceylan v. Turkey, App 23556/94; Sener v. Turkey, App 26680/95; Surek v. Turkey, App 24122/94.
15. Sener v. Turkey, App 26680/95

8 Speaking of terror
or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.

2. Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

The convention also includes important protections. Article 12 requires that the adoption and implementation of the convention by nations “are carried out while respecting human rights obligations, in particular the right to freedom of expression, freedom of association and freedom of religion” under the ICCPR, ECHR and other international treaties. The laws must also be “subject to the principle of proportionality, with respect to the legitimate aims pursued and to their necessity in a democratic society, and should exclude any form of arbitrariness or discriminatory or racist treatment.”

The Convention also excludes the defence of “political offences”. Under Article 20, extradition and mutual legal assistance cannot be refused “on the sole ground that it concerns a political offence or an offence connected with a political offence or an offence inspired by political motives.”

There are concerns that the Convention will be expansively used by some national governments to justify severe restrictions on free expression. Some, such as Russia, which already has controversial laws on extremism, have actively embraced it while adopting legislation that is significantly more far reaching. The CoE review of national laws said that it expected the implementation of the law “will, inevitably and undoubtedly” lead to challenges under the ECHR.

Cybercrime Convention and Optional Protocol on Xenophobia and Racism

In 1997 the CoE formed a Committee of Experts on Crime in Cyber-space (PC-CY). The convention text was finalised in September 2001. After the terrorist attacks on the United States, the convention was positioned as a means of combating terrorism. A signing ceremony took place in November 2001 where it was signed by 30 countries. The convention came into force on 7 January 2004.

The convention has three parts. Part I proposes the criminalisation of online activities such as data and system interference, the circumvention of copyright, the distribution of child pornography, and computer fraud. Part II requires ratifying states to pass laws to increase their domestic surveillance capabilities to cater for new technologies. This includes the power to intercept Internet communications, gain access to traffic data in real-time or through preservation orders to ISPs, and access to data. The final part of the treaty requires all states to co-operate in criminal investigations.

Overall, parts II and III have been the most controversial. Part II of the convention calls for an expansion of technological means to facilitate interception but does not include substantive limitations on its scope or use. This has led to the justification of adopting acts in member states with very broad laws (see Section VI on surveillance) which has profound effects on freedom of expression. This was especially a concern since the convention was intended to be open to non-CoE signatories who were not subject to ECHR protections of human rights. In Part III, civil society campaigners expressed concern over the lack of requirement of dual criminality, believing that it could lead to misuse of cybercrime laws to limit media and criticism by baseless charges. In October 2004, two UK servers for Indymedia, an independent media organisation, were seized at the request of US authorities on behalf of Swiss and Italian authorities.

In addition to the convention, an optional protocol on Xenophobia and Hate Speech was introduced in 2002. The protocol prohibits the dissemination of racist speech including threats and insults and denial and justification of genocide. There have been many calls to use this protocol expansively to ban incitement and glorification related information.

18. Mikhail Kamynin, the Spokesman of Russia’s Ministry of Foreign Affairs, Answers Questions from Interfax News Agency Regarding Deposition by Russian Minister of Foreign Affairs Sergey Lavrov with Council of Europe Secretary General Terry Davis of Russia’s Instrument of Ratification of the CoE Convention on the Prevention of Terrorism, 19 May 2006.
20. CoE Convention on Cybercrime, Treaty No. 185
22. Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS 189.

Effects of international bodies on Council of Europe member states 9
The European Union

The European Union (EU) role in developing anti-terrorism policy has often been considered more controversial than other international bodies. There are likely three reasons for this: One is the more expansive requirements that many of the instruments adopted have favoured compared to those adopted by the CoE. A second factor is the mandatory nature of the instruments which can be enforced by infringement proceedings or cases brought to the European Court of Justice (ECJ). Finally, the process under which various instruments have been adopted has generally been non-transparent. The European Union has been extremely active under the 3rd Pillar (Justice and Home Affairs) in the promoting of enhanced law enforcement powers to fight crime and terrorism which is not subject to the same controls and Parliamentary oversight as other areas of EU activity.

A few weeks after the September 11 attacks, The EU Council proposed the adoption on a framework decision on terrorism to introduce EU-wide definitions of terrorism and criminal sanctions. The Framework decision defines terrorist offences and requires that EU member states criminalise inciting terrorism offences. The Framework Decision was finally adopted in June 2002.

The Decision was strongly criticised for potentially criminalising protests at meetings such as the G-8. It only included a limited recognition of human rights while not imposing any substantive limits on countries. Declaration 10 stated that “Nothing in this Framework Decision may be interpreted as being intended to reduce or restrict fundamental rights or freedoms such as the right to strike, freedom of assembly, of association or of expression” while Article 1(2) noted that the decision “shall not have the effect of altering the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the Treaty on European Union.”

In 2006 the European Commission began examining amending the Framework Decision “in order to devise effective solutions towards fighting terrorist propaganda though various media”. The Commission determined that EU and national legislation needed enhancement. It considered that the Framework Decision “appears to be outdated” and because of the CoE and UN efforts in the field, the EU needed to catch up.

The amendment generally adopts the CoE convention provisions on public provocation, recruitment and training. It defines public provocation as:

the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of one of the offences listed in Article 1(1)(a) to (h), where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed;

The amendment has been strongly criticised for lacking the protections on human rights incorporated into Article 12 of the CoE Convention (see above). The original version introduced by the Commission had no protections and the EU was generally resistant to recognise any problems. The Eurojust representative defended the approach in one hearing stating that “judges and prosecutors will always obey the rule of law and respect the human rights imperatives” so no additional protections were required while a French Senator said “we must stick to general formulations and trust the judge".

The amendment was approved by the Commission in November 2007 and approved by the Council of the EU in April 2008. A revised version was issued by the Council in July 2008. The criticisms led to the adoption of the new section on freedom of expression. It currently states:

This Framework Decision shall not have the effect of requiring member states to take measures in contradiction to fundamental principles relating to freedom of expression, in particular freedom of the press and the freedom of expression in other media as they result from constitutional traditions or rules governing the rights and responsibilities of, and the procedural guarantees for, the press or other media where these rules relate to the determination or limitation of liability.

However, this still raises problems as many of the protections are only non-binding declarations and it only focuses on traditional media issues while ignoring freedom of association and free speech in the religious context.

The European Parliament voted overwhelmingly in September 2008 to revise the draft to remove references to “provocation” and replace them with “incitement”.

32. Email communication from Statewatch, September 2008.
and include new protections on freedom of expression, association, private communications and specifically protect public debate on “sensitive political questions, including terrorism”. The response of the Council and the Commission to the amendments is pending as of the writing of this report.

**Data Retention**

The EU has also been active in the promotion of enhanced surveillance capabilities by member states. The most controversial has been in the area of data retention which requires that member states adopt laws to routinely monitor the Internet and telephone use of all users without a need to find that they are engaged in any illegal activities.

In 2002 the EU introduced amendments to the pending Directive on Privacy and Electronic Communications to allow member states to adopt measures to require that logs of telecommunications activities including telephone, mobile, location data and internet usage be kept for certain periods of time even in the absence of a belief that the users are engaged in criminal activities. Previously, under a 1997 Directive, the data was required to be eliminated as soon as the need for it was done.

In 2006 the European Union adopted the Directive on Data Retention that requires telecommunications providers to automatically collect and retain all information on all users’ activities. The Directive requires member states to require communications providers to retain communications data for a period of between 6 months and 2 years. Member states had until September 2007 to transpose the requirements of the Directive into national laws and until March of 2009 for internet data. The Directive is currently being challenged by the Irish government in the European Court of Justice. A coalition of civil liberties groups have asked the court to find it incompatible with Article 8 and Article 10 protections under the ECHR.

---


III. Limits on access and gathering information

New efforts on counter-terrorism by member states also resulted in new limits on the ability of journalists to gather information. However, at the same time, other pressures have lead to greater openness by governments.

On the positive side, laws mandating the right of individuals to demand information from governments have spread across the Council of Europe member states in the past decade. Today, only a handful of countries have not adopted comprehensive laws on access to information and a CoE working group is nearly complete with developing the world’s first international treaty on the subject.

At the same time, laws on state secrets and criminal codes are also widespread and allow for restrictions in access to information in the name of national security. The scope of these laws have been expending in many nations. There have been an increasing number of cases in the past seven years of these laws being used to prosecute journalists and whistle-blowers.

There is also a growing development in limits on public photography and access to proceedings.

Access to Information Laws

Relevant Standards of the Council of Europe

Access to information is recognised as a human right in Article 10 of the European Convention on Human Rights and has been widely taken on as an administrative tool across the member states of the CoE. Nearly all countries have adopted national legislation and a majority have adopted it as a constitutional right. All but a handful of (40 out of 47) CoE member states have adopted national laws on access to information. These range from the world’s first act in Sweden and Finland in 1766 to Macedonia, which adopted a law in 2006.

Thus far, the European Court of Human Rights has only found in favour of a limited right of access to information under Article 8 (personal privacy) when the information is necessary to protect the requestor’s personal or family life. The Court has also regularly found in favour of a right of access by individuals under Article 8 to their own information held by government bodies including those created by intelligence services.

The efforts of the Council of Europe have been of particular importance in promoting access to information (ATI) laws. The CoE Parliamentary Assembly first issued a resolution in 1979 recognising the importance of access and calling on the Committee of Ministers to recommend that member countries adopt ATI laws.

In 1981, the Committee of Ministers set out general principles implementing a right of access that member countries were recommended to adopt.

In 2002 the Committee of Ministers issued detailed guidelines for member countries on developing access laws. The recommendations have a number of exemptions that would apply in cases relating to anti-terrorism:

37. The only states without national access to information laws are Andorra, Cyprus, Luxembourg, Malta, Monaco, Russia, San Marino. A number of other states’ laws are considered less than effective including Greece, Italy and Spain.


41. Recommendation No. R (81) 19 on the access to information held by public authorities.

Recent Trends

Development in the area of access to information laws has generally been positive in the past seven years. Concern about terrorism has not stopped member states from adopting Freedom of Information (FOI) laws. In that time frame, a number of CoE member states have adopted laws. On their face, these laws appear as open as laws adopted previously. In many cases, the laws include important provisions such as public interest tests that make documents, including those relating to national security, more available than older laws.

A review of laws adopted after 2001 does not find that there is an increased secrecy in the definition of state secrets. Indeed, as with the 2002 CoE Recommendation and draft convention, the trend towards more limited state secrets exemptions in FOI appears to be continuing.

In addition, many countries have amended their laws to improve access. In Norway, an entirely new act was adopted in 2007 which gives broader access to information. In Greece, amendments to the law clarified that all persons were able to ask for information, not just those with a personal interest. Hungary adopted several amendments to improve the use of the law in fighting corruption and extending it to electronic records and system. Other countries including Latvia and France adopted amendments as part of implementing an EU Directive on the reuse of information to improve their access.

Only a few legislative efforts which might have a negative effect on existing access rights have been identified:

- In Ireland, the Freedom of Information Act 1998 was amended in 2003 to remove the requirement that harm must be shown before information can be withheld for defence or national security reasons. However, the police force (Garda Síochána) which also functions as an intelligence service has still not been included in the FOI.

- In Switzerland, a parliamentary committee is investigating why documents relating to an investigation into nuclear smuggling to Libya were shredded by the government.

- In the UK, documents relating to potential fire hazards at a nuclear power plant are being withheld.

- In Sweden, local authorities classified the plans for the new house of the Prime Minister, claiming security.

- A provision in the pending UK Counter-terrorism bill would allow for public and media access to coroner’s inquests to be restricted when “the Secretary of State has certified that the inquest will involve the consideration of material that should not be made public in the interests of national security, the relationship between the United Kingdom and another country, or otherwise in the public interest.”

It is possible, and perhaps likely, that the effects may be more subtle. In the Netherlands, there have been no legislative changes to the Government Information (Public Access) Act (Wet Openbaarheid van Bestuur or WOB) relating to national security or anti-terrorism. However, experts report that there are more subtle difficulties in obtaining some documents that were available before. For example, risk maps to evaluate environmental hazards were taken off the Internet in 2006.

There are some reported incidents on additional secrecy:

- In Sweden, local authorities classified the plans for the new house of the Prime Minister, claiming security.

- In the UK, documents relating to potential fire hazards at a nuclear power plant are being withheld.

- In Switzerland, a parliamentary committee is investigating why documents relating to an investigation into nuclear smuggling to Libya were shredded by the government.

So far, counter-terrorism efforts do not appear to have significantly affected the general right of access to information of European citizens as has happened in the United States. It is likely that given its long history of freedom of information, the US has a more established system of access and users who expect access than most CoE countries, which have only relatively recently adopted laws. Another possible factor is that the exemptions in access laws for national security and separate state secrets laws (see following section) are far broader in most European countries and thus there is not a per-

47. E-mail communication from Roger Vleugels, 1 September 2008.
49. “Plans for PM’s house to be kept secret”, The Local, 29 April 2005.
exception by government officials that this needed to be changed in a significant way.

Another possible factor is that, unlike in areas relating to freedom of expression, there have not been significant international efforts to limit access to information and anti-terrorism legislation has generally not directly limited access. Whereas a number of international instruments on counter-terrorism action specifically try to describe with limits to freedom of expression, there have not been similar instruments that include limits to freedom of information in the counter-terrorism context.

State Secrets Legislation

All CoE member states have legislation on the protection of national security-related secrets. In most countries, the protections are found in the criminal codes and prohibit the unauthorised disclosure of information that is determined by officials to be secret for national security reasons including relating to terrorism. Many countries, especially in Central and Eastern Europe, have adopted more detailed laws which set out categories of information that is eligible for protection and procedures for its protection and access.

Relevant Standards of the Council of Europe

The European Court of Human Rights has decided on the liability of journalists for obtaining and publishing secret information in several cases. Generally it has ruled that Article 10 of the ECHR does not exempt journalists from liability for violating criminal law. However, the Court has more recently noted that “greatest care” needs to be taken when determining the need to punish journalists who publish material in breach of confidentiality when doing so in the public interest. In 2006 the Court ruled that the conviction of a journalist for making a routine inquiry to obtain non-sensitive confidential information in several cases. Generally it has overruled a ECtHR panel decision and ruled that there is no violation of Article 10 in a case where a journalist who had published sensationalised excerpts of an inflammatory memorandum from the Swiss Ambassador on the negotiations over assets of Holocaust victims.

In other jurisdictions outside the CoE member states with similar legislation, there has been a recognition of the problems of the broad scopes of the laws.

Recent Trends

There has been a significant trend in the increased use of state secret laws to penalise whistle-blowers and journalists who publish information of public interest. A review in 2007 by the Organization for Security and Co-operation in Europe (OSCE) found that nearly half of its 56 participating States imposed legal liability for journalists who obtained or published classified information. A 2006 review by the CoE Parliamentary Assembly found many national laws were problematic due to their broad scope and lack of limitations:

A 2006 review by the CoE Parliamentary Assembly found many national laws were problematic due to their broad scope and lack of limitations:

The Assembly notes that legislation on official secrecy in many Council of Europe member states is rather vague or otherwise overly broad in that it could be construed in such a way as to cover a wide range of legitimate activities of journalists, scientists, lawyers or other human rights defenders. In 2007 the Assembly called on member states to amend their laws to ensure that secrecy was not excessive and prone to abuse:

1.1.1. examine existing legislation on official secrecy and amend it in such a way as to replace vague and overly broad provisions with specific and clear provisions, thus eliminating any risks of abuse or unwarranted persecutions;
1.1.2. apply legislation on official secrecy in a manner that is compatible with freedom of speech and information, with accepted practices for international scientific co-operation and the work of lawyers and other defenders of human rights;
1.2. look into ways and means of enhancing the protection of whistle-blowers and journalists, who expose corruption, human rights violations, environmental destruction or other abuses of public authority, in all Council of Europe member states;

56. In Canada, the Ontario Court of Justice ruled in October 2006 that the Security of Information Act which is based on the UK Official Secrets Act was overbroad and disproportionate because it failed to define what was an official secret. Canada (Attorney General) v. O’Neill, 2004 CanLII 41197 (ON S.C.), (2004), 192 C.C.C. (3d) 255.
58. Resolution 1551 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets.
59. Recommendation 1792 (2007) Fair trial issues in criminal cases concerning espionage or divulging state secrets.
60. OSCE Representative on Freedom of the Media, Access to information by the media in the OSCE region: trends and recommendations: Summary of preliminary results of the survey, 30 April 2007.

Limits on access and gathering information
• In Denmark, two journalists and the editor of Berlingske Tidende were prosecuted under the Criminal Code in November 2006 after publishing material leaked from the Defence Ministry revealing that there were doubts over the existence of weapons of mass destruction in Iraq before the invasion, which the government of Denmark supported. The court found they had acted in the public interest in publishing the information and acquitted them.

• In Croatia, journalist Zalko Peratovic was detained and his house searched in October 2007 for violating state secrets after publishing a story on war crimes on his blog. TV Nova station was also raided. The raid was criticised by President Stjepan Mesic. The Parliamentary Council for the Control of Secret Services found that he and five other journalists’ rights had been violated when previously the intelligence agency briefed the president and the media that he was working with foreign intelligence agencies.61

• In Bulgaria, website opasnite.net was shut down by the State Agency for National Security (SANS) in September 2008 for allegedly posting classified information about corruption. A journalist was detained for a day. Another journalist who was reportedly associated with the site was severely beaten by four men a few weeks later.

• In Romania, six journalists were questioned and two were arrested in February 2006 for receiving classified information on military forces in Iraq and Afghanistan from a former soldier. The journalists did not publish the information and handed over the information to the government. The Supreme Court ordered the release of one journalist after she had been detained for two days.

• In the UK, Neil Garrett of ITV News was arrested in October 2005 and detained several other times under the Official Secrets Act after publishing internal police information on the mistaken shooting of Jean Charles de Menezes in a counter-terrorism operation. The story revealed that in an effort to deflect criticism, the police had misled the public about de Menezes’ actions before he was shot. Police were forced to pay extensive damages after they searched the office and home of the Northern Ireland editor of the Sunday Times in 2003 after he published a book that contained transcripts of phone calls intercepted by the security services illegally. The Police Ombudsman described the raid as “poorly led and … an unprofessional operation”. In November 2005, the government threatened to charge several newspapers with violating the Act if they published stories based on a leaked transcript of conversations between PM Tony Blair and President George Bush about bombing Al Jazeera television.

• In Germany, prosecutors announced in June 2007 that they had opened investigations against 17 journalists for violating state secrets after publishing stories on a Parliamentary investigation of the German intelligence agency’s role in CIA anti-terror efforts. All of the cases were dropped in December 2007. Police raided the offices of the magazine Cicero in 2005 and charged the editor with violating state secrets. The Constitutional Court ruled in February 2007 that the police search and seizure was unconstitutional.65

• In Switzerland, three Sonntags Blick reporters were prosecuted in 2007 under the military penal code for publishing an Egyptian government fax confirming the existence of EU-based secret prisons run by the US government. The journalists were acquitted by a military court in April 2007.

There has also been an increase in new laws on state secrets in Central and Eastern Europe. New members of EU and the North Atlantic Treaty Organization (NATO) have adopted these laws on protection of classified information as a condition for joining the organisations.64 This has led to conflicts with access to information laws where nations have adopted provisions not required by the international agreements.64

• In the Czech Republic, the Parliament approved amendments to the law on classified information in 2008 to restrict access to all unclassified NATO and EU sourced information. The government said it adopted the bill due to EU requirements.65

• In Moldova, the government proposed a draft Law on State Secret in 2008 that would allow officials to classify information as “Restricted” if the official finds that the release “cannot be in the favour of the interests and/or security” of the country. Information under that category can be classified for 5 years.

• In Bulgaria, the 2002 Law for the Protection of Classified Information revoked the 1997 Access to Documents of the Former State Security Service Act and Former Intelligence Service of the General Staff Act.

• In Albania, the government proposed amending the existing Law on State Secret in 2006 to include a new “Restricted” category when “unauthorised exposure may damage the normal state activity and the interests or effectiveness of the state institutions.”66 The amendment was eventually limited to only national security cases.

• In Croatia, the Information Security Act adopted in 2007 sets no limits on the duration that state secrets can be classified.67

62. 1 BvR 338/06; 1 BvR 2045/06, 27 February 2007.
63. See NATO, Security within the North Atlantic Treaty Organisation (NATO), Document C-M(2002)49, 17 June 2002. This document was kept non-public for several years by both NATO and national governments while being cited to justify new state secrets acts.
Efforts to expand secrecy laws are not just limited to Central and Eastern European (CEE) countries. Proposals have also been heard in a number of West European countries. The record again has been mixed, with a tension between civil society and intelligence services leading to both increases and decreases in secrecy:

- In the UK, following a series of leaks, the government proposed extending the Official Secrets Act to make it easier to successfully prosecute whistle-blowers. However, this was considered extremely controversial and thus far no public proposals have been introduced.
- In France, a decree was issued in 2003 that broadly classified all information about nuclear power including transport and safety as classified defence information. After protests, it was withdrawn and replaced in 2004. A new law on nuclear transparency was adopted in 2005. In May 2006, a spokesman for an environmental group was arrested for possessing a document on power plant safety.
- In Italy, following a series of scandals involving the secret services, a new law adopted in 2007 on secret service and intelligence limits the imposition of state secrets to 15 years (with possibility of renewal for another 15) and its application to information on terrorism that contravenes constitutional order.

**Limits on Photography**

In many countries, there is increased scrutiny and restrictions on photography, both by professionals and amateurs. Most of these efforts appear to be done without legal authority and include the detaining and assaults of journalists who are taking photos of notable events, such as public protests, the forced deletion of their photographs, or the seizure of photographs for use in prosecutions.

- In the UK, there are no legal restrictions on the photography in public spaces. However, there are widespread reports that police are challenging photographers in public places and at public events and deleting photographs claiming terrorism restrictions. It is also being imposed in private spaces such as shopping malls, which are prohibiting people from taking casual shots. The Home Secretary has acknowledged that there is no legal basis for the stops but has allowed local police to continue to do it.
- In Azerbaijan, journalist Afgan Mukhtarli taking photographs of a protest outside the Russian embassy was detained in August 2008. Police demanded a written explanation from him on why he was there.
- In Montenegro, police detained journalists and seized cameras in October 2008 during a public protest. The cameras were returned later with the photographs deleted.
- In Russia, a number of reporters were arrested during the G-8 meeting in 2006. Two student photographers were detained for several days before being expelled. A reporter with Focus was detained and had his photographs deleted by police after taking a picture of 4 of the G-8 delegates.
- In Spain, authorities seized the cameras of Dutch photographer Joel Van Houdt who was investigating illegal immigration in the Canary Islands. He is being forced to testify in a legal case.
- Some restrictions may be in place in existing state secrets and espionage statutes. In Switzerland, in 2003, the government charged the editor of *SonntagsBlick* under the Military Code for publishing photos of an underground bunker. He was convicted in 2004 and sentenced to 10 days jail but the decision was annulled in 2006 by the highest military court. In Greece, 14 “plane spotters” from the UK and the Netherlands who travelled to a public air show and took photos of military planes were arrested and spent several months in police custody.

72. The European Federation of Journalists is currently conducting a survey of its national members to better evaluate the current trends and problems.
Speaking of terror jail. They were charged as spies and convicted. An appeals court overturned their case in 2002. A number of journalists were detained in 2004 for photographing a port.

There are also increased restrictions on photography in airports. In France, photography in certain areas is prohibited by a 2005 decree. In London, photographers were banned from Heathrow airport during a terror alert.

IV. Limits on freedom of expression

The right to free expression faces significant challenges due to new counter-terrorism efforts. The most significant challenge is from the creation of new crimes for speech that is seen to encourage, either directly or indirectly, terrorism. Restrictions have expanded from existing prohibitions on incitement to much broader and less defined areas such as glorification or “apology” for terrorism. Some countries have adopted broad prohibitions on other speech critical of national institutions and symbols. Internet-based speech has also been affected with attempts to block or remove websites with controversial material.

Political commentary and debate on major issues of the day, such as discrimination against certain ethnic or political groups, autonomy and other issues, is being treated as supporting of terrorism and is banned. Newspapers are shut down, journalists are detained, searches, arrested and tried, and web sites are blocked.

The efforts towards new broader restrictions on speech have mostly been initiated by countries where there are existing, often violent, controversies over territorial issues. Following the events of 11 September and the bombings in London and Madrid, the restrictions have been extending region-wide. They are driven by international instruments by the CoE, EU and UN.

Relevant Council of Europe Standards

The Council of Ministers in their 2007 guidelines on protecting freedom of expression and information in times of crisis recommended that:

Member states should not use vague terms when imposing restrictions of freedom of expression and information in times of crisis. Incitement to violence and public disorder should be adequately and clearly defined."

The European Convention on Human Rights provides for strong protections on freedom of expression under Article 10 while allowing states to protect national security. However, many of the new national laws appear to be in violation of the requirements of the ECHR by stretching the allowable justifications permitted by the European Court of Human Rights. National security and the fight against terrorism are often invoked to justify repressions of protected speech.

The Court has heard numerous cases relating to freedom of expression and national security/anti-terrorism. The case-law of the ECtHR on incitement is not entirely straightforward. The Court has found that incitement can be prohibited under Article 10 in limited circumstances, which are highly context based. The Court attempts to determine if the intent of the speaker was to incite violence based on a number of factors. These include the method of communication, the language used for both the contested speech and previous statements, the size of the audience, and the position and background of the speaker. Within this context, the Court has ruled that purely political speech is protected unless there is a compelling reason for restricting it. However, in October 2008 the Court ruled a fine imposed for a cartoon published a few days after the 11 September attacks which appeared to support it was not a violation of Article 10 in part because of the short time from the incident made it more likely it would provoke violence.

The ECtHR has also generally found that journalists should not be found responsible for reporting the words of others in a responsible way. In a 1994 case, the Court said that: “The punishment of a journalist for assisting in the dissemination of statements made by another person in an interview would seriously hamper the contribution of the press to discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so.”

There is an increasing trend by member states to criminalise speech which could be considered to be supporting of terrorism. As discussed in Section II, international instruments developed by the CoE, EU and UN have pushed member states towards adopting these limitations.

The most common crime prohibited and perhaps the least controversial on its face is incitement. Incitement is typically defined as the direct promotion of criminal acts with the intent of inspiring another person, who may not be known to the speaker, to commit the act. Incitement has been long banned by member states as a general criminal law. The instruments have encouraged member states to adopt specific incitement provisions relating to terrorism.

A review by the CoE in 2004 found that all member states had laws on incitement as part of their criminal codes and a handful had specific provisions on incitement of terrorism.

Many of the laws do not require the actual crime to have been attempted or committed. In Belgium, the Criminal Code was amended by an anti-terrorism act in 2003 to include incitement. It now states:

Any person who, either by views expressed in meetings or public places or by writings, printed matter, images or emblems of any kind displayed, distributed, sold or put on sale or public view, directly provoked others to commit the crime or offence, without prejudice to the penalties imposed by law on authors of provocations to commit crimes or offences, even if such provocations were not acted upon.

As shown by the ECHR case-law discussed above, even the more narrowly defined incitement laws have raised questions when applied to media. There are a number of cases, which might therefore raise concern:

• In Azerbaijan, opposition editor Eynulla Fatullayev was convicted of inciting terrorism and sentenced for 8 ½ years for an article opposing Azerbaijan’s support of US policies relating to Iran. He was previously imprisoned for criminal libel.

• In Austria, Danish cartoonist Jan Egesborg was arrested and had his materials seized for putting up posters in the Vienna underground which criticised Russian President Putin on the death of Russian journalists by prominently placing the words “shoot” and “Putin” on the poster.

More controversial is the adoption of laws on “glorification”, “apologia” or “public promotion” of terrorism. Since the adoption of the CoE Convention on the Prevention of Terrorism, a number of additional member states have adopted glorification laws including Andorra, Lithuania, Russia and the UK.

Of primary concern is the problem of defining what is to be prohibited. The Convention appears to take a narrow approach in prohibiting “public provocation” which is defined as “the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed.” However, while developing the Convention, the CODEXTER committee focused on glorification and apologia which it defined as the “public expression of praise, support or justification of terrorists and/or terrorist acts” and that discussion has continued. The Explanatory Memorandum suggests that “such a provision could cover the dissemination of messages praising the perpetrator of an attack, the denigration of victims, calls for funding for terrorist organisations or other similar behaviour which could constitute indirect provocation to terrorist violence.”

As noted by the CoE working group when developing the Convention, “it is to be expected that the introduction in member states of the Council of Europe of specific anti-terrorism legislation along these lines will, inevitably and undoubtedly, give rise to complaints under the ECHR.” A number of jurisdictions have used the latitude given to countries under the Convention to adopt broad, vaguely defined laws which can be used to seriously limit speech of those opposed to government policies.

In Russia, the 2006 anti-terror law criminalises as a terrorist activity the “popularisation of terrorist ideas, dissemination of materials or information urging terrorist activities, substantiating or justifying the necessity of the exercise of such activity.” Organisations, including media organisations, that are found liable under the act can be liquidated. A second 2006 law that implements the CoE Convention amended the mass media laws to prohibit “distributing materials, containing public appeals to exercising terrorist activity, or justifying terrorism publicly, other extremist materials”. The law also prohibits journalists from discussing counter-terrorism operations. A third law adopted in 2006 extends the definition of extremism to include “Public defamation of the person, deputy public office, the Russian Federation or public office, subject of the Russian Federation, in the performance of their duties or in connection with their performance.” There have
been numerous cases brought against newspapers, commentators, artists, civil society organisations and others under these laws.  

The UK Anti-Terrorism Act 2006 prohibits the direct or indirect encouragement of terrorism. The section states:

For the purposes of this section, the statements that are likely to be understood by members of the public as indirectly encouraging the commission or preparation of acts of terrorism or Convention offences include any statement which:

(a) glorifies the commission or preparation (whether in the past, in the future or generally) of such acts or offences; and

(b) is a statement from which those members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances.

Concerns have been raised over its application to historical events such as Irish independence or the anti-Apartheid campaigns of the 1970s and 1980s as well as current debates over terrorism. The UN Human Rights Committee in 2008 called for the revision of the law because of its vagueness:

The Committee notes with concern that the offence of “encouragement of terrorism” has been defined in section 1 of the Terrorism Act 2006 in broad and vague terms. In particular, a person can commit the offence even when he or she did not intend members of the public to be directly or indirectly encouraged by his or her statement to commit acts of terrorism, but where his or her statement was understood by some members of the public as encouragement to commit such acts.

In France, the 1881 Law on Freedom of the Press prohibits the advocacy of terrorism by means of “speeches, shouts or threats proffered in public places or meetings, or by written words, printed matter, drawings, engravings, paintings, emblems, pictures or any other written, spoken or pictorial aid, sold or distributed, offered for sale or displayed in public places or meetings, either by posters or notices displayed for public view, or by any means of electronic communication.”

Some countries have more general prohibitions on supporting criminal violations. In Germany, the Criminal Code states that whoever “publicly, in a meeting or through dissemination of writings...and in a manner that is capable of disturbing the public peace, approves of one of the unlawful acts named....after it has been committed or attempted in a punishable manner” can be imprisoned for up to three years. In Poland, the Criminal Code penalises any person who “publicly praises the commission of an offence.”

Some countries have adopted provisions that go beyond incitement and glorification to insults of victims of terrorism. In Spain, the Criminal Code was amended in 2000 to prohibit glorification but also “the commission of acts tending to discredit, demean or humiliate the victims of terrorist offences or their families.”

Punk band Soziedad Alkoholika was charged with glorification and degradation of victims in 2006 for publishing songs which criticised the police. The Supreme Court ruled in 2007 that their lyrics did not glorify terrorism or degrade victims and the criticism was protected.

In Lithuania, the 2004 amendments to the Criminal code now punish “Any person who by public oral or written statements or using mass media encouraged or incited an act of terror or other crimes related to terrorism or despised the victims of terror.”

Many countries also protect national symbols. In Turkey, the Terrorism Act and the Criminal Code have provisions to punish anyone who “publicly humiliates the Turkish Flag or the Turkish National Hymn”, “discouraging people from joining the Armed forces” or denigrating the memory of founder of the modern Turkish state, Ataturk. A new section was adopted in the 2006 Anti-terrorism Act which prohibits publication of propaganda such as quoting or discussing the policies of groups such as the PKK. Journalist Cengiz Kapmaz was convicted and sentenced for 10 months under the new section on disseminating propaganda in September 2008. Popular singer Bulent Ersoy is currently being prosecuted for violating the provision on discouraging people from serving in the armed forces.

A provision on “denigrating Turkishness” was amended to limit its application and lower penalties in 2008. Until its amendment, it was used against authors such as Nobel Laureate Orhan Pamuk, scholars and others who raise controversial issues such as Kurdish and Armenian relations. However, there are reports that the revised section is still being applied in a controversial manner.

The UN Special Rapporteur has expressed concern over the broadness of the laws and its application, noting “elements both in the Anti-Terror Act and in the Penal Code which may put severe limitations on the legitimate use of freedom of expression.”

103. Criminal Code §140(2).
104. Criminal Code §253(3).
106. Sentencia Tribunal Supremo núm. 656/2007 (Sala de lo Penal, Sección 1), de 17 julio 2007.
108. Article 300.
109. Article 318.
111. Article 301.
expression of opinions critical of the Government or State institutions, on the forming of organisations for legitimate purposes, and on the freedom of peaceful assembly.”  

In France, the 2003 internal security law prohibits the insult of the flag or the national anthem at a public event. It was adopted after the national anthem was booed by foreign supporters at a football match attended by President Chirac. Laws relating to prohibitions on racist speech have also been broadened in some countries. A review by the CoE Venice Commission in 2007 found that nearly all CoE member states had adopted laws prohibiting incitement to hatred on racial, national and religious grounds.

While the concept is widely supported, some have been used in cases which raise significant free expression concerns:

- Police asked the Crown Prosecution Service and broadcast regulator Ofcom to investigate if Channel 4 had incited hate by broadcasting the “Undercover Mosque” show revealing that several preachers were encouraging violence and discrimination against non-Muslims. Both found that there was no legal violation and the police were forced to apologise and pay £100,000 damages to Channel 4 in 2008.
- In the Netherlands, cartoonist Gregorius Nekschot was arrested and detained for over a day in May 2008 after a complaint about cartoons published in 2005. The arrest led to an emergency debate in Parliament. The hearing revealed that the Ministry of Justice had set up a secret special inter-departmental working group to monitor cartoonists.
- In Russia, government prosecutors found that an episode of American cartoon South Park was a violation of the extremism law for inciting racial hatred in September 2008 and recommended that the license of 2X2, the broadcaster be withdrawn. The license was renewed and the channel has appealed the extremism decision to court but has taken 12 shows including South Park and The Simpsons off the air.

Possession of terrorist materials

Countries are also increasingly adopting laws that prohibit the possession of terrorist materials. The danger with these kind of laws is that it can also apply to journalists or scholars who collect the information to better understand the mind-set of the terrorists.

In the UK, the Terrorism Act 2000 prohibits the possession of information that would be useful to commit a terrorist act. The Court of Appeals ruled in 2008 that the law required that the information must not just encourage terrorism but must provide practical assistance.

The Court of Appeals in 2008 also threw out the case of the “lyrical terrorist” who had written provocative poems and slipped them to people at Heathrow Airport. She was charged with having terrorist manuals on her hard drive but the case was dropped after the police admitted that they could not prove that she had the intent to commit acts. In 2008 two researchers at Nottingham University were arrested after one downloaded an al-Qaeda training manual for his thesis. He was detained for 6 days and released. The other is now in jail facing deportation from the UK.

The 1939 Irish Offenses Against the State Act prohibits the possession of “any treasonable document, seditious document, or incriminating document in his possession or on any lands or premises owned or occupied by him or under his control.” Journalists are required to turn it over the Garda upon request or face prosecution. Four BBC reporters were detained under Section 30 of the Act in 2008 while they were investigating members of the Provisional IRA. They were later released without charge.

In Cyprus, the draft anti-terrorism bill will also make the possession of seditious documents a terrorist offence.

Effects on Internet Speech

In the past decade, the effect of the Internet on media and freedom of expression has been dramatic. Most newspapers and other media outlets have Internet sites which make information available. New media organisations that are only Internet-based have sprung up. New forms of media such as blogging and social networks allow millions to publish information quickly and at low or no cost.

119 “Moscow prosecutors say South Park cartoons could incite hatred”,RIA Novosti. 8 September 2008.
120 R v K [2008] All ER (D) 188 (Feb).
121 R v Malik [2008] All ER (D) 201 (Jun).
123 Offence Against the State Act 1939, §12.
Relevant Council of Europe Standards

In March 2008 the Committee of Ministers of the Council of Europe adopted Recommendation CM/Rec (2008) 6 to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters. In the guidelines appended to the Recommendation, the Committee of Ministers states that member states should:

i. refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10, paragraph 2, of the European Convention on Human Rights, as interpreted by the European Court of Human Rights;
ii. guarantee that nationwide general blocking or filtering measures are only introduced by the state if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights.

Counter-terrorism efforts have also affected access to Internet-based information sources. There is grave concern in many countries about the use of the Internet for “cyber-terrorism” – attacks on Internet sites such as government and corporate sites, networks and critical infrastructure such as power plants that are connected online, and also the use of the Internet by terrorists to recruit, plan acts, and send out propaganda. The response to these concerns has been increased efforts by authorities to limit access to their sites. This can be either the shutting down of sites if they are within the jurisdiction of the country or another country that will support their efforts or setting up technical measures to block access from users inside the country.

The EU in 2007 launched a programme called the “Check the Web” to increase the monitoring Islamist web sites across the EU, co-ordinated by Europol. The proposal called for a co-ordinated review and actions on sites noting that “numerous Internet sites in a wide variety of languages must be monitored, evaluated and, if necessary, blocked or closed down.” Thus far, very little information on the programme has been released about how many sites have been identified and blocked or shut down.

In Turkey, a law on Internet crimes was adopted in 2007 that allows the blocking of websites by a court order if the content in question is hosted in Turkey. Additionally, the law enables the Telecommunications Communication Presidency to issue administrative orders to block access to websites which are hosted outside the Turkish jurisdiction. As of August 2008, 853 websites including major international sites with millions of users including YouTube, Geocities, dailymotion, and Wordpress have been blocked recently for violations of the laws on terrorism, insulting Turkishness, defamation, and other crimes listed in Article 8 of Law No. 5651. 241 of the 853 websites are blocked by court orders, while the majority (612) are blocked by administrative orders issued by the Presidency.

In Russia, a bill is pending which would extend the laws on mass media to nearly all Internet sites and subject them to stricter regulations. Current extremism laws are already used against Internet-based sites. According to the government, over 1,000 sites were banned in 2007. ingushetiya.ru was banned by a court in May 2008 for extremism. Magomed Yevloyev, the owner of the site, was shot dead in a police car in September 2008.

In the UK, the Terrorism Act 2006 requires Internet providers to remove materials that promote or glorify terrorism. Providers are not liable if “upon obtaining actual knowledge that the information was unlawfully terrorism-related, the service provider expeditiously removed the information or disabled access to it.” Home Secretary Jacqui Smith announced in January 2008 that she was meeting with Internet Service Providers to develop a plan to block sites promoting terrorism.

In France, the French government announced in June 2008 that they had reached an agreement with Internet Service Providers to block sites that contain terrorist, racist and pornographic content by 2009. Individuals are encouraged to submit sites for blocking.

Blocking systems that have been created for other reasons have been proposed to extend to terrorism material. In Finland, a law adopted in 2006 that was supposed to only cover child pornography has already been used to block a site that was critical of the government body that is in charge of it and has been proposed to be extended. In Norway, a system that blocks access

125.Recommendation CM/Rec (2008) 6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters.
126.Council of the EU, Council Conclusions on cooperation to combat terrorist use of the Internet “Check the Web”, Document 8457/07 ENFOPOL 9496/06 ENFOPOL 9 JAI 261, 18 May 2006.
128.Council of the EU, Proposals of the German Delegation regarding EU co-operation to prevent terrorist use of the Internet (“Check the Web”), Document 8457/07 ENFOPOL 9496/06 ENFOPOL 9 JAI 261, 18 May 2006.
130.“Russian police actively engaged in closing extremist websites”, Interfax (via BBC Monitoring), 7 May 2008.
131.“France to blacklist Web sites”, Associated Press, 10 June 2008.
135.“France to blacklist Web sites”, Associated Press, 10 June 2008.
to sites accused of possessing child pornography was set up by ISP Telor in 2004. In 2007, a government commission (Datakrimutvalget) proposed extending the blocking more materials including terrorism materials. The proposal was rejected by the government.
V. Protection of journalists’ sources and materials

It is well established that journalists’ sources are crucial to freedom of expression. Journalists are often given information with the expectation that they will not identify the source who could be fired, arrested or harmed if their roles are revealed. The information given has been kept from the public as it is often classified, sensitive, private or embarrassing.

Journalists also collect information by interviewing a variety of people for information, making notes, recording, and taking photographs or video. Generally it is understood by all involved that the journalists are independent parties who are attempting to inform the public about issues that are of a public interest, not acting on behalf of police or other government agencies.

Nearly all Council of Europe member states have explicit legal recognition of the right of journalists to protect their sources which is underpinned by decisions of the European Court of Human Rights.

At the same time, the ECtHR and many national laws authorise the overriding of this protection for investigating serious crimes, such as terrorism. Some countries have also adopted new anti-terrorism or crime laws which give broad powers to authorities to obtain documents or information from all persons.137

Even in the presence of the strong protections of the ECHR, Council of Europe normative texts and national laws, there have been many cases in member states where journalists have been detained and newspapers searched to identify sources. Broad security laws have often been used against journalists to force them to disclose their sources. The following are a few security-related cases in recent years:

- In the UK, Manchester police used powers under the Terrorism Act 2000 to demand that journalists from the Sunday Times, BBC, CBS and other news outlets give all information about a former terrorist that they had interviewed. Author Shiv Malik was required to disclose copies of his notebooks after a court reduced the amount of information he was required to disclose.
- In France, journalist Guillaume Dasquie was detained for two days in December 2007 after he published an article in Le Monde that quoted from French intelligence documents indicating that they were aware of plans to hijack planes prior to the 9/11 attacks. The authorities demanded that he disclose the identity of sources or face charges of violating state secrets law.
- In Turkey, weekly Nokta was raided and had its equipment searched and journalists questioned in 2007 after it published materials about plans for a military coup and stories about military blacklisting of journalists.138 The magazine was shut down by its owners afterwards and the editor was prosecuted for libel while two others were charged with inciting disrespect against the military.
- In the Netherlands, journalists Bart Mos and Joost de Haas from the newspaper De Telegraaf were imprisoned in November 2006 after refusing to testify in court about the source of intelligence dossiers on a criminal that they published. They were released by a higher court after two days detention.139
- In Russia, the offices of Permsky Obozrevatel newspaper and homes of its journalists in Perm were searched several times in 2006 and 2007, on various charges including that they were violating the state secrets law.
- In Italy, police searched the offices of La Repubblica and the Piccolo newspapers and two journalists’ homes and seized files following stories about Italy’s role in the 2003 kidnapping of Egyptian cleric Osama Moustafa Hassan Nas. In 2002 and 2004, police and anti-terrorism officials raided the offices and homes of journalists who were investigating...
police and anti-terrorism abuses at the 2001 G-8 meeting in Genoa.

- In Germany, echoing a similar case in the 1960s that led to major reforms and improvements in press freedom, Cicero magazine and a journalist’s home were raided and searched in 2004 after it published an article quoting a federal criminal police document on an al-Qadida leader. The Constitutional Court ruled in February 2007 that searches of a newsroom violated the Constitutional protections on freedom of the press. The Court found that the mere publication of a state secret without other evidence is not sufficient to accuse the journalist of violating state secrets protections and that a search to identify a source is not constitutionally permissible.

Relevant Council of Europe Standards

The ECtHR has decided in numerous cases that the protection of sources is a crucial part of freedom of expression. The Court has found that “Protection of journalistic sources is one of the basic conditions for press freedom... such a measure cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest.” Any restrictions on protection of sources “call for the most careful scrutiny by the Court”. These protections also extended to searches of journalists’ offices and homes to discover the source of information to a story which violated both Article 10 and the journalist’s Article 8 right of privacy. It also found that imprisoning journalists to force them to disclose their sources is a violation of Article 10.

In 1994 the European Ministerial Conference on Mass Media Policy called for recognition of sources noting that it “enables journalism to contribute to the maintenance and development of genuine democracy”. In 2000 the CoE Committee of Ministers adopted a Recommendation with detailed principles on protection of sources that all member states should incorporate into national law. It describes the principles as “common European minimum standards concerning the right of journalists not to disclose their sources of information.” The guidelines recommend that nations authorise disclosure only “if circumstances are of a sufficiently vital and serious nature.”

The explanatory memorandum to the Recommendation lists the circumstances where the disclosure is necessary as ‘the protection of human life’, ‘the prevention of major crime’, ‘the defence in the course of legal proceedings of a person who is accused or convicted of having committed a serious crime’. Major crime is defined as “murder, manslaughter, severe bodily injury, crimes against national security, or serious organised crime”.

The Council of Europe has given special recognition to the need for protection of sources in conflicts and other dangerous circumstances. In 1996, the CoE Committee of Ministers called on member states to ensure the confidentiality of sources in “situations of conflict and tension”. The CoE reaffirmed the need for protection in these situations in 2005 with a declaration which called upon member states not to undermine protection of sources in the name of fighting terrorism, noting that “the fight against terrorism does not allow the authorities to circumvent this right by going beyond what is permitted by [Article 10 of the ECHR and Recommendation R (2000) 7]”.

The Committee of Ministers in September 2007 issued “Guidelines on protecting freedom of expression and information in times of crisis” which recommended that member states adopt the 2000(7) recommendations into law and practice and further recommended that:

With a view, inter alia, to ensuring their safety, media professionals should not be required by law-enforcement agencies to hand over information or material (for example, notes, photographs, audio and video recordings) gathered in the context of covering crisis situations nor should such material be liable to seizure for use in legal proceedings.

Council of Europe Member States Protections

The vast majority of countries in Europe have adopted some form of protection of sources legislation. Over 40 countries have adopted a provision in their criminal or civil codes, media laws or other laws while others recognise it in their case-law.

There has been a steady trend towards adoption of protections into law following the cases in the European Court of Human Rights. In the past few years, new laws have been adopted in many countries including Bel-

---

140. Decision BvR 538/06; 1 BvR 2045/06, 27 February 2007.
143. Stokkuil v. the Netherlands, Application No. 64752/01 (22 November 2007).
146. Declaration on freedom of expression and information in the media in the context of the fight against terrorism, 2 March 2005.
147. Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis, adopted by the Committee of Ministers on 26 September 2007 at the 1005th meeting of the Ministers’ Deputies.
148. See OSCE, Access to Information by the Media in the OSCE Region, April 2007.
gium, Georgia, Luxembourg, Monaco, Switzerland, and Turkey.

Most laws have limitations on information that is classified as national security related.

- In Belgium, the protections can be overridden by a judge in cases relating to terrorism or serious threats to the physical integrity of a person, if the information is of crucial importance and cannot be obtained any other way.\textsuperscript{150}

- In Luxembourg, under the 2004 Law on the Freedom of Expression in the Media, journalists can be forced to disclose a source where it involves the prevention of crimes against individuals, drug trafficking, money laundering, terrorism or state security.\textsuperscript{151}

- In the UK, the protection of sources can be overridden if it is “established to the satisfaction of the court that disclosure is necessary in the interests of justice or national security or for the prevention of disorder or crime.”\textsuperscript{152}

- In France, a new sources bill pending before the Parliament would require disclosure of information in “exceptional cases, if the nature and seriousness of the crime or offence to which it relates as well as the necessity of investigations warranted [this].”\textsuperscript{153}

New anti-terrorism laws in several of the member states give authorities broad powers to demand information from any person with very little procedural protections compared to traditional search and seizure powers under the criminal law.

In the UK, the Terrorism Act 2000 gives authorities broad powers to demand journalistic materials in terrorism investigations if there are reasonable grounds for believing that “the materials is likely to be of substantial value...in a terrorism investigation” and if it is “in the public interest” that access should be given because of “the benefit likely to accrue”.\textsuperscript{154} The request must be approved by a circuit judge.

The law has been used a number of times to demand materials from journalists who investigated or interviewed terror suspects.\textsuperscript{155} In 2008 the Court of Justice ruled that an author could be forced to give up copies of materials gathered directly from the suspect but did not have to give up materials gathered from other sources.\textsuperscript{156}

In France, a 2003 law on criminality brought in to fight serious crime and terrorism requires that journalists hand over documents or face significant fines.\textsuperscript{157}

In Germany, the pending “Law on the prevention of threats of international terrorism” will substantially limit the protection of sources. It is being strongly opposed by the journalist, newspaper, magazine and broadcaster associations.\textsuperscript{158}

Some jurisdictions also have imposed duties on individuals, including journalists, to proactively disclose information about security related threats. Some of these laws have been used against journalists.

- The UK Terrorism Act creates a criminal violation for not revealing information about an act of terrorism.\textsuperscript{159} In the Malik case, the government refused to immunise the author while forcing him to disclose the information, thus potentially subjecting him to prosecution for violation of the law for not handing over his notes. The Court refused to hear the argument.

- In Russia, journalist Yelena Masyuk from NTV was threatened with a violation of the criminal code provisions on failure to report a crime and reporting a fugitive after she interviewed Chechen leader Shamil Basayev in 1995.\textsuperscript{160}

- In Hungary, if a source discloses a state secret to a journalist, the journalist must inform the authorities or face criminal penalties themselves.\textsuperscript{161}
VI. Wiretapping and surveillance of journalists

Laws, policies and technologies relating to interception of communications and other forms of telecommunications surveillance have undergone substantial changes since 2001. Countries have increasingly been adopting laws that give them broad powers to conduct surveillance. Generally, the laws do not contain specific limits on the use of the powers against the media. The result of these changes has been an increase in the use of surveillance against journalists for both national security and non-national security related reasons.

This area is of strong interest to journalists. Sources are less likely to come forward if they believe that they can be identified or located through their telecommunications. In some cases, governments have attempted to manipulate news coverage when they have inside information on pending stories.

The surveillance is usually conducted in secret so journalists are not aware of the intrusion and it cannot be challenged or limited. Claims by governments that these intrusions are necessary for national security often make it difficult for there to be any public examination or oversight of the information that is being collected and the legitimacy of the collection.

Throughout CoE member states, there is a worrying trend in the use of both authorised and unauthorised electronic surveillance to monitor journalists by governments and private parties to track their activities and identify their sources. Most of these cases are unrelated to countering terrorism but are authorised under the broad powers of national laws or even done illegally, in order to identify who a journalist has received information from.

- In Germany, a parliamentary report released in 2006 revealed that the Federal Intelligence Agency (BND) had been illegally spying on journalists, including placing spies in newsrooms for over a decade to identify sources and monitor what newspapers were working on. The BND was ordered to stop spying on journalists. However, less than a year later, the BND was revealed to have spied on journalists in 2006 and 2007 who were writing stories on Afghanistan.\textsuperscript{162}
- In Belgium, the mobile phone of journalist Anne de Graaf from De Morgen was monitored for two months in 2004 to identify her sources after she wrote a story about a meeting to discuss anti-terrorism threats in Antwerp. The Court of First Instance ruled in 2007 that the interception was illegal because it was insufficient grounds to conduct surveillance to identify her source and awarded her 500 euros.\textsuperscript{163}
- In the Netherlands, the government monitored the telephones of journalists from the newspaper De Telegraaf who had received and published classified information that revealed that a criminal kingpin was obtaining confidential information from police and intelligence agencies while still in jail. The tap was approved by the Supreme Court in September 2008 and is now being appealed to the European Court of Human Rights. In November 2007 a government department admitted that it had used the password of a former employee to access the computer system of news agency GPD to identify what stories were going to be run.\textsuperscript{164}
- In Denmark, police monitored the telephones of journalist Stig Matthiessen from Jyllands-Posten after he began investigating the existence of a “death list” but refused to identify his sources.\textsuperscript{165} The taps were later found by a court to be unlawful.
- In the Czech Republic, two journalists in 2006 were among the many persons wiretapped in a bid to reveal who had leaked classified information about organised crime connections with the civil service.\textsuperscript{166}

\textsuperscript{162} “German Spies Caught Reading Journalist’s e-mails”, Deutsche Welle, 21 April 2008.
\textsuperscript{163} “L’Etat belge condamné pour une écoute sur une journaliste”, L’Express, 13 July 2007.
\textsuperscript{165} “Police tap journalist’s phone”, The Copenhagen Post, 6 September 2002.

Wiretapping and surveillance of journalists 29
**Relevant Council of Europe Standards**

The limits on interception of communications flow from international, regional and national protections on human rights. Of primary importance is Article 8 of the European Convention on Human Rights on the right to private life. In addition, there is some recognition of the importance of Article 10. The European Court of Human Rights has long recognised that interception of communications is a violation of Article 8 for all citizens.\(^1\)

The ECtHR requires that member states that wish to intercept communications must adopt laws that are “particularly precise” in the types of conditions that interfere with Article 8 will be conducted. It has established a set of minimum safeguards relating to the categories of crimes, duration of taps, precautions on communication of the information and circumstances on deletion. The law must also ensure that there are “adequate and effective safeguards against abuse”.

The balancing between investigating and fighting terrorism with intrusive techniques and privacy and other rights was discussed in the first ECtHR case from 1978 on wiretapping in a terrorist investigation. The court said that countries were given a wide margin of applicability in the use of the techniques but also said:

The Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.\(^2\)

In the past two years, the Court has heard a number of cases on interception powers relating to national security and terrorism.\(^3\) In two of the cases, the court found that the laws did not provide sufficient safeguards and thus the laws violated Article 8. In one of the cases, the ECtHR recognised that interception of communications could violate Article 10 rights to freedom of expression, especially if they were used to identify a journalist’s sources.\(^4\) It concluded that for the intrusion to be justified, the monitoring needed to be limited, not done for the purpose of identifying sources, and subject to strict safeguards and oversight.

The 2000 Council of Europe Recommendation on protection of sources proposes strict limits on the use of surveillance on journalists.\(^5\) Principle 6 states that “interception orders or actions concerning communication or correspondence of journalists or their employees” should not be applied if “their purpose is to circumvent the right of journalists, under the terms of these principles, not to disclose information identifying a source” and any of these techniques has been used, that the “measures should be taken to prevent the subsequent use of this information as evidence before courts”.

However, only a few countries have adopted legislation that specifically limits the use of surveillance to identify sources or other protected materials from journalists. The Belgian law on protection of journalists’ sources only allows detection or investigative methods when it is authorised by a judge under the same limits as forcing the disclosure of a source.\(^6\) In Austria, “Employees of media services” are protected under the media law from interception of their communications in the course of their work.\(^7\) In Georgia, it is a criminal offence to intercept journalists communications for the purpose of violating professional secrets.\(^8\) In France, a pending bill on sources would extend protections to “indirect attacks”.

**Increased Powers for Interception and Investigation**

All Council of Europe member states allow the use of electronic surveillance to investigate serious crime. Typically, the countries require that an independent court or magistrate approve a request to investigate a serious crime. Often, interceptions for national security purposes such as terrorism investigations are subject to less requirements and oversight. The laws must as a minimum follow the protections as set out by the European Court of Human Rights.

---

6. 171 Recommendation No. R (2000) 7 of the Committee of Ministers to member states on the right of journalists not to disclose their sources of information.
7. 172. Loi relative a la protection des sources journalistes, §5.
into account human rights concerns and the requirements of the evolving case-law of the ECtHR.

Following the 2001 terrorist attacks, many CoE countries have adopted new laws or expand the use of old laws to monitor communications. These laws expand surveillance in a number of ways:

1) extending the range of crimes that interception is authorised for;
2) relaxing legal limitations on approving and conducting surveillance including allowing for warrantless interception in some cases;
3) authorising the use of invasive techniques such as Trojan horse and remote keystroke monitoring to be used;
4) greater demands for identification of users of telecommunications services.

Some of the recent legislation adopted to extend interception:

• In Sweden, a 2008 law authorises the National Defence Radio Establishment (Försvarets Radioanstalt – FRA) to monitor without a court order all telecommunications that cross the borders of the country via cable or wireless.176 The agency would be able to data mine the communications. This will have a significant effect because due to the nature of modern telecommunications networks, a significant proportion of domestic communications crosses national borders and will be subject to interception. Following massive public protests, amendments are currently being considered.

• In Russia, a 2006 anti-terrorism law allows authorities in an anti-terrorist operation to “exercise control over telephone communications and over other information transmitted over telecommunication channels, as well as searching in electric communication channels and in postal mailing for the purpose of detecting information concerning the circumstances of committing an act of terrorism and the persons who have prepared and committed it, as well as for the purpose of preventing other terrorist acts”.177 An amendment in 2007 extends the justification for interception to “moderately serious crimes” which includes extremism offences.178

• In the Netherlands, the Intelligence and Security Services Act adopted in 2003 gives the intelligence services broad powers to intercept wireless communications that cross the border and retain them.179 The Act allows the use of “special powers” such as interception against people who, while not the subject of investigations, are related to the target. Dutch courts and the internal oversight body have approved the use of this measure against journalists to identify the source of leaked documents.180

• The Slovenian Intelligence and Security Agency Act was amended in 2003 to allow for interception for terrorist, organised crime and also disclosure of state secrets to foreigners.181 It requires telecommunications providers to “provide conditions to enforce special judicially-approved forms of data acquisition.”

• In Germany, the G-10 Law allows warrantless automated wiretaps of international communications by the Intelligence Service (BND) for purposes of preventing terrorism. The Federal Constitutional Court ruled in 1999 that it did not have enough protections and violated the rights of privacy and free speech. It was amended in 2001 to include better supervision and was upheld by the ECtHR in 2007.182 However, as the cases above show, there are serious questions about the adequacy of the supervision in practice.

Authorities are also increasing their abilities to break into target computers to install special monitoring software. In Germany, the state of North-Rhine Westfalia adopted a law allowing for remote searches and computer spyware in 2006. The Federal Constitutional Court found the law unconstitutional in 2008.183 The anti-terror bill currently being considered at the German federal level would allow for government agents to use spyware and remote surveillance in criminal investigations.184 In Denmark the “Anti-Terror Package” introduced in October 2001 and approved in June 2002 gave law enforcement the power to secretly install snooping software on the computers of criminal suspects.185 The software will record keystroke data and transmit it electronically to the law enforcement agency.

176 Proposition 2006/07:63.
180 See Supervisory Committee on the Intelligence and Security Services, Report On the investigation by the AIVD into the leaking of state secrets, CTIVD No. 10, 15 November 2006.
184 See Joint Statement on a draft law on prevention of threats of international Terrorism by the Bundeskriminalamt (BKA Law), 11 September 2008.
185 Act No. 378, 6 June 2002.
Increasing Technical Capabilities to Intercept

Another important trend is the increasing legal requirements to ensure that all telecommunications equipment is designed to facilitate interception of communications. These require that technical capabilities for interception be built into telecommunications equipment. The requirements originally only applied to telephones, but now are being extended to Internet and other new technologies.

Under the new capabilities, the process is now typically automated. In some jurisdictions, the interception is solely under the control of government officials who install “black boxes” in telephone providers systems to allow for access. In others, the systems are designed into the system by the manufacturer by companies such as Siemens and Ericsson.186

The trend began long before the 2001 attacks. In the United States, the Communications Assistance for Law Enforcement Act (CALEA) was adopted in 1994.187 Following its adoption, US officials met with their European counterparts and the EU Council and secretly adopted a framework recommendation in 1995.188

The CoE Cybercrime Convention, which was approved in 2001, incorporated these proposals, and requires that countries adopt laws to authorise the interception of content and traffic data and ensure that communications providers adopt technical means to ensure surveillance.189 The Convention has now been ratified by 24 countries.

Many states have adopted laws to implement these regulations. In the UK, the Regulation of Investigatory Powers Act 2000 (RIPA) adopted in 2000 requires public Communications Service Providers to provide a “reasonable” interception capability in their networks.190 In Belgium, a law adopted in December 2001 bans telecommunications providers from giving anonymous communications.191 The Slovenian Electronic Communications Act adopted in 2004 requires that “Operators shall be obliged at their own expense to ensure adequate equipment and appropriate interfaces enabling lawful interception of communications in their networks”.192

In other countries, government controlled systems are installed at the communications providers’ office to conduct surveillance. In Russia, the government in 1998 began to require that all ISPs install devices that are directly connected to government offices to allow monitoring.193 A similar system was set up in Ukraine in 2002 under an order from the State Committee on Communications.194 The order was declared to be unlawful in 2005 but reportedly is still in operation.

The automated nature of the systems raises concerns about the interceptions of communications approved and executed without adequate oversight. Traditionally, when a wiretap was to be conducted, it was necessary to provide a written authorisation to a third party, such as the telecommunications provider. If automated systems bypass that process, it will be able to conduct unsanctioned surveillance. As the number of legal and illegal intercepts continues to rise, checks are crucial to ensure that abuses do not occur.

The new surveillance capabilities may also make it easier for unauthorised persons to intercept communications. In Greece, it was discovered in 2006 that unknown persons had broken the security of cell phone operator Vodafone and used the built-in surveillance capabilities of the Ericsson equipment to tap the communications of over 100 prominent people including Prime Minister Costas Karamanlis and several journalists.195 Several investigations have not been able to identify who conducted the intercepts. In Italy, the transcripts of widespread illegal taps and surveillance of journalists, sports figures and politicians were leaked to the press in 2006.196

Increased Collection and Use of Telecommunications Records

Related to the surveillance of communications is the increased collection of transactional information by telecommunications companies. These records can be used by authorities to gather a detailed record of the activities of journalists including who their sources are. The records are also often the target of law enforcement who use them to identify the identity or location of sources, even in non-serious cases.

In 2003 the Irish police demanded access to phone records of journalists after they published stories that a minister’s son had been assaulted.197 The Guardi said that they needed the information to discover if someone had violated the Official Secrets Act in disclosing the information to the media. The technique was described as believed to now be “standard practice” when information was leaked to the media. The 2005 Criminal Jus-

---

186. See e.g. “Snoop software makes surveillance a cinch”, New Scientist, 23 August 2008.
189. art. 21, 22.
In recent trends which have greatly accelerated since the attacks is the requirement by governments asking telecommunications providers to automatically collect and retain all information on all users’ activities including details about e-mails sent and received, web sites visited, and instant messages. Mobile telephone companies are required to collect information on calls and messages sent and received including the location of the person when they make calls.

While the subject had been discussed for a few years prior, only a few countries had adopted requirements because of concerns over privacy and cost. The CoE discussed and rejected including it in the Convention on Cyber-crime.

Following the 11 September attacks, countries began to quickly adopt the requirements. In the UK, the Anti-terrorism, Crime and Security Act (ATCS) adopted December 2001 allowed the Home Secretary to issue a code of practice for the “voluntary” retention of communications data by communications providers for the purpose of protecting national security or preventing or detecting crime that relates to national security. Most communications providers began to retain data. In Denmark, the 2002 “Anti-Terror Package” required the retention of communications data for up to 2 years. The 2002 Spanish law on e-commerce required that traffic data be kept for 12 months. In Ireland, the 2005 Criminal Justice (Terrorist Offences) Act requires that telecommunications providers retain data for three years.

This requirement will shortly be mandatory EU-wide. The 2006 EU Directive on Data Retention requires all EU member states to adopt rules on data retention and to allow for collecting and holding information for up to two years. To date, over a dozen countries in Europe have fully implemented the Directive. In the UK, consultation is currently pending that would require that all traffic data including internet usage and mobile location data be kept for one year. The government is now reportedly considering proposals for creating a national database of all communications data.

In Germany, data retention requirements were adopted in 2007 requiring that data be retained for six months, following a challenge filed by 30,000 citizens, the Federal Constitutional Court in March 2008 issued a preliminary ruling that the data retention law is unconstitutional in giving too much access which should only be limited to serious crimes when no other means of obtaining the information is available.

In Ireland, the 2005 Criminal Justice (Terrorist Offences) Act requires that telecommunications providers retain data for three years.

This information is also being used by private organisations against journalists. In Germany, Deutsche Telekom was discovered in 2008 to be monitoring the records of journalists and board members to identify who was providing information to journalists. In Finland, the five employees of telecommunications company Sonera were convicted in 2005 of illegally obtaining the phone records of two journalists from Helsingin Sanomat and employees of the Sonera to discover who was the source of a leak.

Technological advances have substantially increased the amount of information that is available about a person’s activities. Internet usage can create a “digital mirror personality” which reveals significant details about a users professional and personal life and activities including their email contacts, social networks and web searches and browsing. Mobile telephones provide detailed records about a user’s location. This transactional data is increasingly being kept on all users for both commercial and national security reasons. It is often subject to lesser protections than interceptions.

198 Irish Daily Mail, June 6, 2008.
200 “Did Deutsche Telekom Spy on Journalists and Board Members?”, Spiegel Online, 26 May 2008.
201 “Five get suspended sentences in Sonera telephone record case”, Helsingin Sanomat, 30 May 2005.
204 See Section II for details.
207 Act establishing new telecommunications surveillance and other covert investigative measures and to implement the Directive 2006/24/EC (BGBl I 2007, p. 3198 ff.).
Increased Requirements for Identification of Mobile and Internet Users

Relating to the issue of retention and use of telecommunications records are requirements for telecommunications providers that only provide for occasional communications services to identify their users and keep records of their activities. These include pre-paid mobile phones and cyber cafes. Journalists often use these services to keep in touch with their sources while not leaving records that can be monitored.

The EU Council issued a conclusion in 2003 that recommended that member states “consider a set of appropriate requirements for tracing the use of prepaid card technology.” A review in 2006 found that a few member states had adopted requirements. The requirements were often ignored or easily bypassed.

- In Switzerland, the wiretap law was amended in June 2004 to require registration of pre-pay phones after which 140 000 phones were disabled.
- In Italy, a decree approved in 2005 required that providers of telecommunications obtain biographical information about their users before allowing them to use their services.
- The Irish government announced in 2007 that it was planning to create a mandatory regime of phone registration to fight drug crime.
- The UK government is planning to require passports or ID cards to get a mobile phone as part of the Communications Data Bill.

These identification requirements have been extended in a few jurisdictions to cyber cafes. In a number of CoE member states, governments have imposed new requirements for the monitoring and identification of users of cyber cafes.

- In Italy, the 2005 decree also requires that all cyber cafes obtain biographical information about their users.
- In France, the 2006 anti-terrorism act requires that cyber cafes, bars and others that offer Internet access to retain data on their users activities and allows the police to obtain the information without a court order for terrorism investigations.
- In Bulgaria, the local authority in the city of Plovdiv issued an order in 2004 requiring that all cyber cafes keep the social security numbers of users, along with their activity records.

These rules are likely to have a chilling effect not just on journalists but on any users that wish to access public or legal, but controversial materials.

209. See Council conclusions on the tracing of the use of prepaid mobile telephone cards, in order to facilitate criminal investigations 7808/03 ENFOPOL 21 OC 130; EU wants identification system for users of prepaid telephone cards, Telepolis, 19 May 2002.
VII. Conclusion

The last seven years have seen many policy and legislative changes which have serious effects on the abilities of journalists to gather and disseminate information. Terrorism is often used as a talisman to justify stifling dissenting voices in the way that calling someone a communist or capitalist were used during the Cold War.

In too many cases, the legislation and policies adopted are disproportionate and appear to be used in abusive ways not to protect public safety and the nation but rather the political interests of governments. Newspapers have been shut down, journalists arrested and jailed, newsrooms searched and spied on and web sites shut down or blocked. Even historically human rights friendly nations have been adopting excessive and disproportionate legislation.

The international bodies have developed unbalanced instruments that do not adequately ensure that human rights are protected. In part, that is because some of the worst national governments are the strongest supporters of expansive international instruments to justify their domestic abuses. The Commission and Council of the European Union have been especially deficient in ensuring that human rights are respected in their proposals relating to anti-terrorism and communications privacy. The Council of Europe’s efforts on anti-terrorism and cyber-crime are not noteworthy for inclusion of human rights concerns either. The organisation’s long-standing reputation as a champion of human rights is challenged by these efforts.

The role of the national courts and the European Court of Human Rights have been unsatisfactory. The national courts have not universally recognised the requirements of the European Convention on Human Rights. The European Court case-law on incitements and publication of secrets has been inconsistent and does not easily set boundaries that countries should follow. Cases take nearly a decade to be decided and remedies are not adequate to ensure the problems will not occur again.

There are some positive trends. Nearly all member states now have legal recognition of the rights of any citizen to demand information from government bodies. Almost all also recognise the fundamental rights of journalists to protect their sources. However, these have also regularly being undermined by security legislation which allows government officials broad discretion to act in the name of fighting terrorism.

The Council of Europe should take leadership of a pro-human rights effort to ensure that national governments and international bodies are respecting human rights. New instruments that promote journalists’ rights should be developed while existing ones should be strengthened or revised.
VIII. Appendix

Guidelines of the Committee of Ministers of the Council of Europe on protecting freedom of expression and information in times of crisis

(Adopted by the Committee of Ministers on 26 September 2007 at the 1005th meeting of the Ministers’ Deputies)

Preamble

The Committee of Ministers,
1. Emphasising that freedom of expression and information and freedom of the media are crucial for the functioning of a truly democratic society;
2. Reaffirming that Article 10 of the European Convention on Human Rights (ETS No. 5) and the relevant case-law of the European Court of Human Rights remain the fundamental standards concerning the exercise of the right to freedom of expression and information;
3. Deeply concerned by the fact that crisis situations, such as wars and terrorist attacks, are still widespread and threaten seriously human life and liberty, and the fact that governments, concerned about the survival of society may be tempted to impose undue restrictions on the exercise of this right;
4. Condemning the killings and other attacks on media professionals and recalling its Recommendation No. R (96) 4 on the protection of journalists in situations of conflict and tension;
5. Recalling Resolution No. 1 on freedom of expression and information in times of crisis adopted by the Ministers of states participating in the 7th European Ministerial Conference on Mass Media Policy (Kyiv, 10-11 March 2005);
6. Having taken note of Resolution 1535 (2007) and Recommendation 1783 (2007) of the Parliamentary Assembly of the Council of Europe on threats to the lives and freedom of expression of journalists;
7. Welcoming Resolution 1738 (2006) of the Security Council of the United Nations condemning attacks on media professionals in conflict situations and recognising the urgency and necessity of taking action for the protection of these professionals;
8. Underlining that dialogue and co-operation between governments, media professionals and civil society can contribute to the efforts to guarantee freedom of expression and information in times of crisis;
9. Convinced not only that media coverage can be crucial in times of crisis by providing accurate, timely and comprehensive information, but also that media professionals can make a positive contribution to the prevention or resolution of certain crisis situations by adhering to the highest professional standards and by fostering a culture of tolerance and understanding between different groups in society,
10. Adopts, as an extension and complement to the “Guidelines on human rights and the fight against terrorism” adopted on 11 July 2002, the following guidelines and invites member states to ensure that they are widely disseminated and observed by all relevant authorities.

I. Definitions

1. As used in these guidelines,
   • the term “crisis” includes, but is not limited to, wars, terrorist attacks, natural and man-made disasters, i.e. situations in which freedom of expression and information is threatened (for example, by limiting it for security reasons);
   • the term “media professionals” covers all those engaged in the collection, processing and dissemination of information intended for the media. The term includes also cameramen and photographers, as well as support staff such as drivers and interpreters.
II. Working conditions of media professionals in crisis situations

**Personal safety**

2. Member states should assure to the maximum possible extent the safety of media professionals – both national and foreign. The need to guarantee the safety, however, should not be used by member states as a pretext to limit unnecessarily the rights of media professionals such as their freedom of movement and access to information.

3. Competent authorities should investigate promptly and thoroughly the killings and other attacks on media professionals. Where applicable, the perpetrators should be brought to justice under a transparent and rapid procedure.

4. Member states should require from military and civilian agencies in charge of managing crisis situations to take practical steps to promote understanding and communication with media professionals covering such situations.

5. Journalism schools, professional associations and media are encouraged to provide as appropriate general and specialised safety training for media professionals.

6. Employers should strive for the best possible protection of their media staff on dangerous missions, including by providing training, safety equipment and practical counselling. They should also offer them adequate insurance in respect of risks to the physical integrity. International organisations of journalists might consider facilitating the establishment of an insurance system for freelance media professionals covering crisis situations.

7. Media professionals who are expelled from zones with restricted access for disobeying national and international law, inciting violence or hatred in the content of their news or spreading propaganda of warring parties should be accompanied by military forces to a neutral, secure region or a country or embassy.

**Freedom of movement and access to information**

8. Member states should guarantee freedom of movement and access to information to media professionals in times of crisis. In order to accomplish this task, authorities in charge of managing crisis situations should allow media professionals accredited by their media organisations access to crisis areas.

9. Where appropriate, accreditation systems for media professionals covering crisis situations should be used in accordance with Principle 11 of the Appendix to Recommendation No. R (96) 4 of the Committee of Ministers to member states on the protection of journalists in situations of conflict and tension.

10. If required by national law, accreditation should be given to all media professionals without discrimination according to clear and fast procedures free of bureaucratic obstacles.

11. Military and civilian authorities in charge of managing crisis situations should provide regular information to all media professionals covering the events through briefings, press conferences, press tours or other appropriate means. If possible, the authorities should set up a secure information centre with appropriate equipment for the media professionals.

12. The competent authorities in member states should provide information to all media professionals on an equal basis and without discrimination. Embedded journalists should not get more privileged access to information than the rest except for the advantage naturally due to their attachment to military units.

III. Protection of journalists’ sources of information and journalistic material

13. Member states should protect the right of journalists not to disclose their sources of information in accordance with Recommendation No. R (2000) 7 of the Committee of Ministers on the same subject. Member states should implement in their domestic law and practice, as a minimum, the principles appended to this recommendation.

14. With a view, inter alia, to ensuring their safety, media professionals should not be required by law-enforcement agencies to hand over information or material (for example, notes, photographs, audio and video recordings) gathered in the context of covering crisis situations nor should such material be liable to seizure for use in legal proceedings. Any exceptions to this principle should be strictly in conformity with Article 10 of the European Convention on Human Rights and the relevant case-law of European Court of Human Rights.

IV. Guarantees against misuse of defamation legislation

15. Member states should not misuse in crisis situations libel and defamation legislation and thus limit freedom of expression. In particular, member states should not intimidate media professionals by law suits or disproportionate sanctions in libel and defamation proceedings.

16. The relevant authorities should not use otherwise legitimate aims as a pretext to bring libel and defamation suits against media professionals and thus interfere with their freedom of expression.
V. Guarantees against undue limitations on freedom of expression and information and manipulation of public opinion

17. Member states should not restrict the public’s access to information in times of crisis beyond the limitations allowed by Article 10 of the European Convention on Human Rights and interpreted in the case-law of the European Court of Human Rights.

18. Member states should always bear in mind that free access to information can help to effectively resolve the crisis and expose abuses that may occur. In response to the legitimate need for information in situations of great public concern, the authorities should guarantee to the public free access to information, including through the media.

19. Member states should not use vague terms when imposing restrictions of freedom of expression and information in times of crisis. Incitement to violence and public disorder should be adequately and clearly defined.

20. International and national courts should always weigh the public’s legitimate need for essential information against the need to protect the integrity of court proceedings.

21. Member states should constantly strive to maintain a favourable environment, in line with the Council of Europe standards, for the functioning of independent and professional media, notably in crisis situations. In this respect, special efforts should be made to support the role of public service media as a reliable source of information and a factor for social integration and understanding between the different groups of society.

22. Member states should consider criminal or administrative liability for public officials who try to manipulate, including through the media, public opinion exploiting its special vulnerability in times of crisis.

VI. Responsibilities of media professionals

23. Media professionals need to adhere, especially in times of crisis, to the highest professional and ethical standards, having regard to their special responsibility in crisis situations to make available to the public timely, factual, accurate and comprehensive information while being attentive to the rights of other people, their special sensitivities and their possible feeling of uncertainty and fear.

24. If a system of embedded journalists needs to be maintained and journalists choose to make use of it, they are advised to make this clear in their reports and to point out the source of their information.

25. Self-regulation as the most appropriate mechanism for ensuring that media professionals perform in a responsible and professional way needs to be made more effective in times of crisis. In this regard, co-operation between self-regulatory bodies is encouraged at both the regional and the European levels. Member states, professional organisations of journalists, other relevant non-governmental organisations and the media are invited to facilitate such co-operation and provide further assistance where appropriate.

26. Media professionals are invited to take into consideration in their work Recommendation No. R (97) 21 of the Committee of Ministers to member states on the media and the promotion of a culture of tolerance and to apply as a minimum the professional practices outlined in the appendix to this recommendation.

VII. Dialogue and co-operation

27. National governments, media organisations, national or international governmental and non-governmental organisations should strive to ensure the protection of freedom of expression and information in times of crisis through dialogue and co-operation.

28. At the national level, relevant stakeholders such as governmental bodies, regulatory authorities, non-governmental organisations and the media including owners, publishers and editors might consider the establishment of voluntary fora to facilitate, through dialogue, the exercise of the right to freedom of expression and information in times of crisis.

29. Media professionals themselves are encouraged, directly or through their representative organisations, to engage in a constructive dialogue with the authorities in situations of crisis.

30. Non-governmental organisations and in particular specialised watchdog organisations are invited to contribute to the safeguarding of freedom of expression and information in times of crisis in various ways, such as:

- maintaining help lines for consultation and for reporting harassment of journalists and other alleged violations of the right to freedom of expression and information;
- offering support, including in appropriate cases free legal assistance, to media professionals facing, as a result of their work, lawsuits or problems with the public authorities;
- co-operating with the Council of Europe and other relevant organisations to facilitate exchange of information and to effectively monitor possible violations.

31. Governmental and non-governmental donor institutions are strongly encouraged to include media
development and media assistance as part of their strategies for conflict prevention, conflict resolution and post-conflict reconstruction.

Declaration on freedom of expression and information in the media in the context of the fight against terrorism

(Adopted by the Committee of Ministers on 2 March 2005 at the 917th meeting of the Ministers’ Deputies)

The Committee of Ministers of the Council of Europe,
Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and promoting the ideals and principles which are their common heritage;
Considering the dramatic effect of terrorism on the full enjoyment of human rights, in particular the right to life, its threat to democracy, its aim notably to destabilise legitimately constituted governments and to undermine pluralistic civil society and its challenge to the ideals of everyone to live free from fear;
Unequivocally condemning all acts of terrorism as criminal and unjustifiable, wherever and by whomever committed;
Noting that every state has the duty to protect human rights and fundamental freedoms of all persons;
Recalling its firm attachment to the principles of freedom of expression and information as a basic element of democratic and pluralist society and a prerequisite for the progress of society and for the development of human beings, as underlined in the case-law of the European Court of Human Rights under Article 10 of the European Convention on Human Rights as well as in the Committee of Ministers’ Declaration on the freedom of expression and information of 1982;
Considering that the free and unhindered dissemination of information and ideas is one of the most effective means of promoting understanding and tolerance, which can help prevent or combat terrorism;
Recalling that states cannot adopt measures which would impose restrictions on freedom of expression and information going beyond what is permitted by Article 10 of the European Convention on Human Rights, unless under the strict conditions laid down in Article 15 of the Convention;
Recalling furthermore that in their fight against terrorism, states must take care not to adopt measures that are contrary to human rights and fundamental freedoms, including the freedom of expression, which is one of the very pillars of the democratic societies that terrorists seek to destroy;
Noting the value which self-regulatory measures taken by the media may have in the particular context of the fight against terrorism;
Bearing in mind the Resolutions and Recommendations of the Parliamentary Assembly on terrorism;
Recalling the Guidelines on Human Rights and the Fight against Terrorism which it adopted on 11 July 2002,
Calls on public authorities in member states:
• not to introduce any new restrictions on freedom of expression and information in the media unless strictly necessary and proportionate in a democratic society and after examining carefully whether existing laws or other measures are not already sufficient;
• to refrain from adopting measures equating media reporting on terrorism with support for terrorism;
• to ensure access by journalists to information regularly updated, in particular by appointing spokespersons and organising press conferences, in accordance with national legislation;
• to provide appropriate information to the media with due respect for the principle of the presumption of innocence and the right to respect for private life;
• to refrain from creating obstacles for media professionals in having access to scenes of terrorist acts that are not imposed by the need to protect the safety of victims of terrorism or of law enforcement forces involved in an ongoing anti-terrorist operation, of the investigation or the effectiveness of safety or security measures; in all cases where the authorities decide to restrict such access, they should explain the reasons for the restriction and its duration should be proportionate to the circumstances and a person authorised by the authorities should provide information to journalists until the restriction has been lifted;
• to guarantee the right of the media to know the charges brought by the judicial authorities against persons who are the subject of anti-terrorist judicial proceedings, as well as the right to follow these proceedings and to report on them, in accordance with national legislation and with due respect for the presumption of innocence and for private life; these rights may only be restricted when prescribed by law where their exercise is likely to prejudice the secrecy of investigations and police inquiries or to delay or impede the outcome of the proceedings and without prejudice to the exceptions mentioned in Article 6 paragraph 1 of the European Convention on Human Rights;
• to guarantee the right of the media to report on the enforcement of sentences, without prejudice to the right to respect for private life;
• to respect, in accordance with Article 10 of the European Convention on Human Rights and with Recommendation No. R (2000) 7, the right of journalists not to disclose their sources of information; the fight against terrorism does not allow the authorities to circumvent this right by going beyond what is permitted by these texts;
• to respect strictly the editorial independence of the media, and accordingly, to refrain from any kind of pressure on them;
• to encourage the training of journalists and other media professionals regarding their protection and safety and to take, where appropriate and, if circumstances permit, with their agreement, measures to protect journalists or other media professionals who are threatened by terrorists;
Invites the media and journalists to consider the following suggestions:
• to bear in mind their particular responsibilities in the context of terrorism in order not to contribute to the aims of terrorists; they should, in particular, take care not to add to the feeling of fear that terrorist acts can create, and not to offer a platform to terrorists by giving them disproportionate attention;
• to adopt self-regulatory measures, where they do not exist, or adapt existing measures so that they can effectively respond to ethical issues raised by media reporting on terrorism, and implement them;
• to refrain from any self-censorship, the effect of which would be to deprive the public of information necessary for the formation of its opinion;
• to bear in mind the significant role which they can play in preventing “hate speech” and incitement to violence, as well as in promoting mutual understanding;
• to be aware of the risk that the media and journalists can unintentionally serve as a vehicle for the expression of racist or xenophobic feelings or hatred;
• to refrain from jeopardising the safety of persons and the conduct of antiterrorist operations or judicial investigations of terrorism through the information they disseminate;
• to respect the dignity, the safety and the anonymity of victims of terrorist acts and of their families, as well as their right to respect for private life, as guaranteed by Article 8 of the European Convention on Human Rights;
• to respect the right to the presumption of innocence of persons who are prosecuted in the context of the fight against terrorism;
• to bear in mind the importance of distinguishing between suspected or convicted terrorists and the group (national, ethnic, religious or ideological) to which they belong or to which they claim to subscribe;
• to assess the way in which they inform the public of questions concerning terrorism, in particular by consulting the public, by analytical broadcasts, articles and colloquies, and to inform the public of the results of this assessment;
• to set up training courses, in collaboration with their professional organisations, for journalists and other media professionals who report on terrorism, on their safety and the historical, cultural, religious and geopolitical context of the scenes they cover, and to invite journalists to follow these courses.
The Committee of Ministers agrees to monitor, within the framework of the existing procedures, the initiatives taken by governments of member states aiming at reinforcing measures, in particular in the legal field, to fight terrorism as far as they could affect the freedom of the media, and invites the Parliamentary Assembly to do alike.
The Council of Europe has forty-seven member states, covering virtually the entire continent of Europe. It seeks to develop common democratic and legal principles based on the European Convention on Human Rights and other reference texts on the protection of individuals. Ever since it was founded in 1949, in the aftermath of the second world war, the Council of Europe has symbolised reconciliation.

Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex

http://www.coe.int/justice/