Controlling Internet Content:
Implications for Cyber-Speech

**International Conference on
Freedom of Expression in Cyberspace**
UNESCO, Paris, France, 3-4 February 2005

Dr. Yaman Akdeniz

**Lecturer in CyberLaw, School of Law, University of
Leeds; Director, Cyber-Rights & Cyber-Liberties (UK)
<http://www.cyber-rights.org>**

Speech/content regulation

- **Illegal vs. Harmful Content**
  - » Separate policy action is required for illegal and harmful content
  - » The difference between illegal and harmful content is that the former is **criminalised by national laws**, while the latter is considered as **offensive or disgusting by some people but certainly not criminalised by national laws**.
- **Illegal Content**
  - » Child Pornography, Hate Speech
- **Harmful Content**
  - » Pornography, Hate Speech
- **Grey areas** – Hate Speech, defamation (competing rights)
- **Responses to Illegal & Harmful Content**
  - » **Government Regulation**
    - – Laws at the national level
    - – Directives, Regulations at the Supranational Level (EU)
    - – Conventions at the CoE (CyberCrime) and UN Level (Optional protocol)
  - » **Self and Co-Regulation**
    - – Development of **Hotlines, Codes of Conduct, Filtering Software, and Rating Systems**

Government Action and Regulation

- **Government Regulation**
- **Illegal Content**
  - » Illegal content often criminalised by national laws
  - » Supranational Harmonisation at the EU level
    - – Council Framework Decision on combating the sexual exploitation of children and child pornography
  - » Regional Harmonisation at the CoE level
    - – CyberCrime Convention
  - » International Harmonisation at the UN level
    - – Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

---

Government Action and Regulation

- **Harmful Content**
  - » Different approaches to "hate speech" in Europe: Illegal, harmful, offensive speech?
  - » This form of Internet content may include **sexually explicit content, political opinions, religious beliefs, views on racial matters, and sexuality**.
  - » **"freedom of expression extends not only to ideas and information generally regarded as inoffensive but even to those that might offend, shock, or disturb"**
  - » **Harm Criterion is different within different European states:** Human Rights and ECHR balance? See *Handyside v UK* (1976), App. no. no. 5493/72, Ser A vol.24, (1976); *Castells v. Spain* (1992), App. no.11798/85, Ser.A vol.236, (1992)
- Problems of harmonisation and concerns for freedom of expression
  - » Regional Harmonisation at the CoE level
    - – Additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems
    - – Not much support

Child Pornography	Hate Speech	Pornography
➢ Society sees it as a problem.	✓ Society sees it as a problem	➢ Society does NOT always see it as a problem
➢ Child pornography is not a new problem.	✓ Racism and xenophobia is not a new problem.	➢ Pornography is certainly NOT new
➢ Digital child pornography is not a new problem - can be traced back to mid 1980s.	✓ Digital hate is not a new problem - can be traced back to mid 1980s.	➢ Difficult to categorise: Depending upon its nature and the laws of a specific state it could be considered illegal or harmful/offensive (BUT legal)
➢ Clear cut example of "illegal "content"	✓ Difficult to categorise: Depending upon its nature and the laws of a specific state it could be considered illegal or harmful/offensive (BUT legal)	➢ Harm criterion is different within different European states.
➢ Criminalised by the CoE CyberCrime Convention, the UN Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and the EU Council Framework Decision on combating the sexual exploitation of children and child pornography (not adopted yet)	✓ Harm criterion is different within different European states. ✓ CoE Additional Protocol to the CyberCrime Convention on the criminalisation of acts of a racist and xenophobic nature committed through computer systems: **23 signatories so far but no ratifications.**	➢ UK approach is rather different to the German or Scandinavian approaches to sexually explicit content ➢ **NO international attempt to regulate "sexually explicit content"**
➢ UN Optional Protocol: **108 Signatories, 71 Parties as of February 2004.**		

Self & Co-Regulatory Initiatives

- ➢ Regulation is often designed to reduce risk **but alternative methods can be less costly, more flexible** and **more effective** than **prescriptive government legislation**. These include the options
  - ➢ "**to do nothing**"
  - ➢ **self-regulation**
  - ➢ **co-regulation**
  - ➢ **information and education campaigns**
- ➢ The CoE Declaration on Freedom of communication on the Internet adopted by the Committee of Ministers of the Council of Europe on 28 May 2003 encouraged self-regulation and co-regulatory initiatives regarding Internet content.
- ➢ Similar recommendations were also made in a CoE Recommendation (2001) 8 on self-regulation concerning cyber-content.
- ➢ The no rush to legislation approach adopted by the European Commission with its Action Plan on promoting safer use of the Internet should be applauded which is now extended to cover EU candidate countries. The Action Plan includes research into technical means to tackle both illegal and harmful content, and information and education campaigns.

Better Policy Making?

State | Private Sector

Civil Society

Problem

- Benefits
- Advantages
- Disadvantages
- Cost
- Effectiveness

Co-operation

Risk Analysis

State Regulation

No Regulation

Governance

Respect for <u>Normative</u> & <u>Process</u> Conditions

<u>Self-Regulation</u>

<u>Information and education campaigns</u>

Co-Regulation

Problems with Self and Co-regulatory initiatives

Generally the outstanding drawback with a self-regulatory arrangement is that

- *it does not apply to those organisations who are not members of the scheme*.
  - » where there is only partial coverage, it is often those who stay outside the scheme who tend to be the main cause of consumer problems.
  - » where there is full coverage across a business or professional sector there can be *a strong tendency towards anti-competitive behaviour*.
  - » There can be *distortion of the market*. Non-members of a self-regulatory scheme do not have to follow the rules, so they can under-cut the market with lower standards.
- A plethora of codes and, often, their inaccessibility make it difficult to *educate participating organisations,* consumers and their respective advisers about their *obligations and right*s.
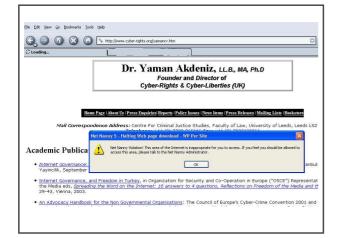

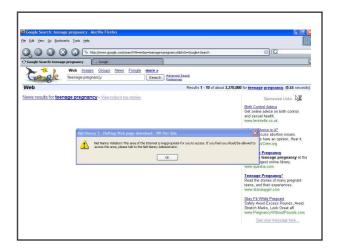## Problems with Self and Co-regulatory initiatives

- *A limited range of sanctions* is available for breach of self-regulatory rules.
  - » **expulsion** (a step a trade association, may be reluctant to take)
  - » **a fine** (which seems rare in practice).
- *Public confidence may be lackin*g
- Problems with **accountability**
  - » There are **real and perceived doubts** about the ability of professional or trade bodies **to both represent the interests of their members and aspire to a public interest role**.
  - » *Doubts about impartiality* **are especially acute** where the self-regulator is responsible for enforcement, or is involved in adjudicating disputes between consumers and traders.
- As with legislation, if there is no commitment and resources for monitoring and enforcement, *effectiveness will be limite*d.

Problems with Rating & Filtering Systems

- Both rating and filtering systems are **problematic**
  - » Originally promoted as technological alternatives that would prevent the enactment of national laws regulating Internet speech, filtering and rating systems have been shown to pose their own significant threats to free expression. When closely scrutinised, these systems should be viewed more realistically as fundamental architectural changes that may, in fact, facilitate the suppression of speech far more effectively than national laws alone ever could. (Global Internet Liberty Campaign, 1999).
- They do **NOT** offer <u>full protection</u> to concerned citizens
- They could be **defective**
- Massive **overblocking** is witnessed in may filtering software
- **Too much reliance on** mindless mechanical blocking through identification of key words and phrases.
- They are based upon the morality that an individual company/organisation is committed to: broad and varying concepts of offensiveness, "inappropriateness," or disagreement with the political viewpoint of the manufacturer is witnessed.
- Apart from overblocking, **underblocking** is also witnessed with certain filtering software

---

Problems with Rating & Filtering Systems

- The capacity of the rating & filtering tools **is limited to certain parts of the Internet**.
- The rating and classification of all information on the Internet is "**impracticable**".
- There is **no consensus** as to what should be filtered or rated.
- **Adults' rights vs. children's rights:** While the children's access is the most cited excuse for the regulation of the Internet, this global medium is not only accessed and used by children.
  - » Any regulatory action intended to protect a certain group of people, such as children, should not take the form of an unconditional and universal prohibition on using the Internet to distribute content that is freely available to adults in other media.
- If a "**light regulatory touch**" with an emphasis on self-regulatory or co-regulatory initiatives represent the European vision, then "**self**" **should mean individuals** rather than self-regulation by the Internet industry without the involvement of individuals and Internet users.
- Parents and teachers and those who are responsible for children's Internet usage need to be educated. **Putting the PC in the living room or installing a filtering software is NOT the solution**.

Problems with Codes of Conduct

Generally
- **Harmonisations is difficult**
  - » Development of Europe wide ISP Codes of Conduct has been problematic
  - » There are different approaches to illegal and harmful content
  - » Each country may reach its own conclusion in defining the borderline between what is permissible (legal) and not permissible (illegal)
  - » It is difficult to draw up a pan-European code which sets substantive limits as to illegal content
- **Market decides**?
  - » Not truly self-regulatory: Governments are involved and slowes down the process
- **ISPs have different relationship with information**
  - » Third party content – they do not want to get involved with policing
  - » Although no ISP controls third party content or all of the backbones of the Internet, the crucial role they play in providing access to the Internet made them visible targets for the control of "content regulation" on the Internet.
- **What happens when there are conflicting rights?**
  - » There are areas which is difficult for the ISPs to decide on issues (e.g. **defamation**)
- **What happens if an ISP does not join or act by the Code**?
  - » Complaint mechanisms hard to develop?

General Principles on Content Regulation by ISPs

- The **primary responsibility** for Internet content rests with the **content providers** and **not with the ISPs**.
- The **ISP must respect freedom of expression** of users and content providers and allow expression to be communicated unless evidently illegal.
- The **right to privacy of online users** of the ISPs should be respected.
- In order to encourage expression and respect for privacy, ISPs should offer positive guidance and facilities to Internet users and content providers.
- ISPs **should not impose any form of monitoring or classification requirements** which are inconsistent with the freedoms and rights of users or content providers.
- ISPs should observe the value of freedom of information in their own activities to the greatest extent possible consistent with commercial interests. It follows that their customers should know:
  - » what codes of practice they operate under
  - » what policies they have internally for refusal/withdrawal of subscriptions
  - » what policies exist for co-operation with law enforcement authorities
  - » any blocking of content activity by the ISPs

A Workable System?

- A credible self and co-regulatory framework could only work if
  - » backed not only by government but also by industry and civil society reps.
  - » **Respect** fundamental human rights such as freedom of expression and privacy
  - » command **public confidence**
  - » there is strong **external consultation and involvement** with all relevant stakeholders in the design and operation of the scheme
  - » the operation and control of the scheme is **separate** from the institutions of the industry (so far as practicable)
  - » consumer, public interest and other **independent representatives are fully represented** (if possible, up to 75 per cent or more) on the governing bodies of self-regulatory schemes.
  - » the scheme is based on **clear and intelligible statements of principle** and **measurable standards** – usually in a Code – which address **real consumer and user concerns.**
  - » the rules **identify the intended outcomes**.
  - » the scheme is **well publicised,** with maximum education and information directed at consumers and users.
  - » the scheme is regularly reviewed and **updated** in the light of changing circumstances and expectations.
  - » It involves an "**independent complaints**" mechanism.