



Internet Freedom: a comparative assessment

Dr Ian Brown
Oxford Internet Institute
University of Oxford



Outline

- General principles from EU telecoms framework and EU/Council of Europe human rights law
- Freedom of expression: web blocking in maintaining public order, child protection and copyright law; holocaust denial and hate speech
- Privacy: Data protection, DPI, and data retention
- Contrasts with the US





UK and EU legal framework

- Communications Act 2003: §3 “General duties of OFCOM (1) It shall be the principal duty of OFCOM, in carrying out their functions—(a) to further the interests of citizens in relation to communications matters; and (b) to further the interests of consumers in relevant markets, where appropriate by promoting competition”; implements Directive (2002/21/EC) on a Common Regulatory Framework
- The Treaty on European Union: §6(3) “Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union’s law.”



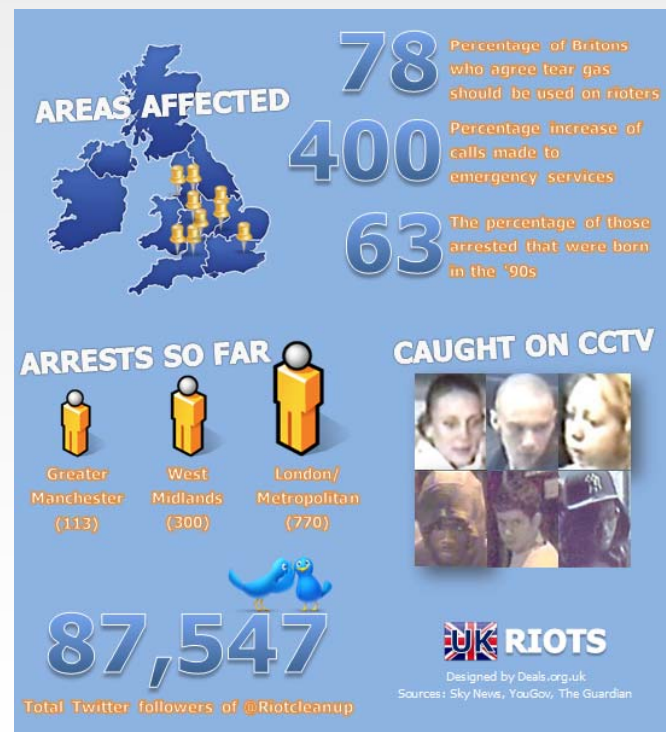
EU Charter of Fundamental Rights

- §7 Everyone has the right to respect for his or her private and family life, home and communications.
- §8 Everyone has the right to the protection of personal data concerning him or her.
- §11(1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.



English riots August 2011

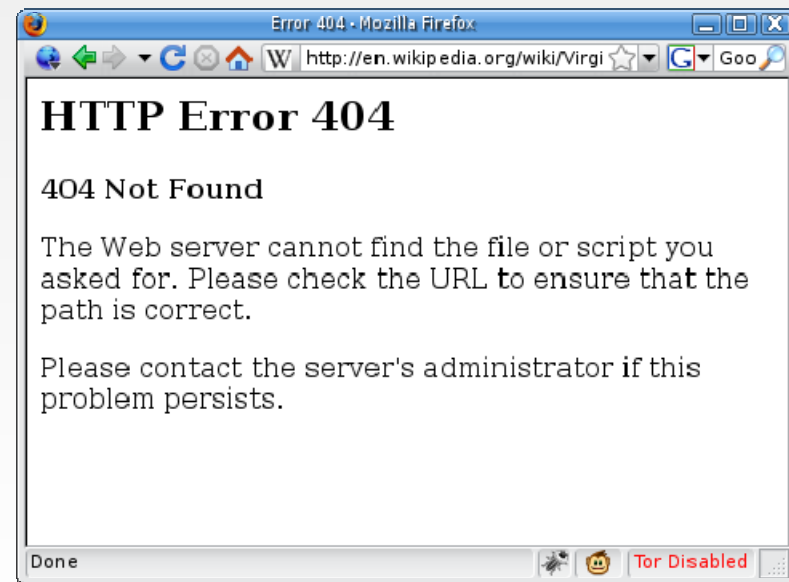
- Riots coordinated using Facebook, Twitter, BBM
- Prime Minister: “We are working with the police, the intelligence services and industry to look at whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality.” (10/8) but “The government did not seek any additional powers to close down social media networks.” (25/8)
- Lord Chief Justice, confirming two 4-year sentences: “the abuse of modern technology for criminal purposes extends to and includes incitement of very many people by a single step... modern technology almost certainly assisted rioters in other places to organise the rapid movement and congregation of disorderly groups in new and unpoliced areas.”





BT Cleanfeed and other web blocking

- “Voluntary” system affecting >98% of retail ISP customers in UK
- Block access to sites listed by self-regulatory Internet Watch Foundation as containing criminal child abuse images
- Now being referenced in other court decisions: would make Newzbin site blocking “modest and proportionate” *20th Century Fox v BT* [2011] EWHC 1981 (Ch)





Blocking v freedom of expression

- Ofcom net neutrality consultation (2010): §2.8 “it is widely accepted that the blocking of illegal content (such as images of child abuse) is necessary and that steps taken to address issues such as online copyright infringement would be viewed as acceptable traffic management.”
- “I want it out - blocking has never helped a single child”. “Lots of organizations have been calling for deletion and furthermore there is no scientific evidence that blocking is effective. With blocking the illegal content is still on the net” “we run the risk of censorship on the Internet” and “we don’t want an infrastructure in Europe which would lead to blocking other material” –Petra Kammerevert MEP



Holocaust denial and hate speech

- Council of Europe Cybercrime Convention optional protocol (ETS 189): “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:”
 - §3(1) “distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.
 - §6(1) “distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity”
- *LICRA v Yahoo!* Tribunal de grande instance, Paris, 2000



Privacy and Deep Packet Inspection

- “I call on the UK authorities to change their national laws and ensure that national authorities are duly empowered and have proper sanctions at their disposal to enforce EU legislation on the confidentiality of communications. This should allow the UK to respond more vigorously to new challenges to e-privacy and personal data protection, such as those that have arisen in the Phorm case. It should also help reassure UK consumers about their privacy and data protection while surfing the internet.” –Commissioner Reding
- “New measures should clarify the practical consequences of the net neutrality principle, as this has already been done in some Member States, and ensure that users can exercise a real choice, notably by forcing ISPs to offer non-monitored connections.” –European Data Protection Supervisor

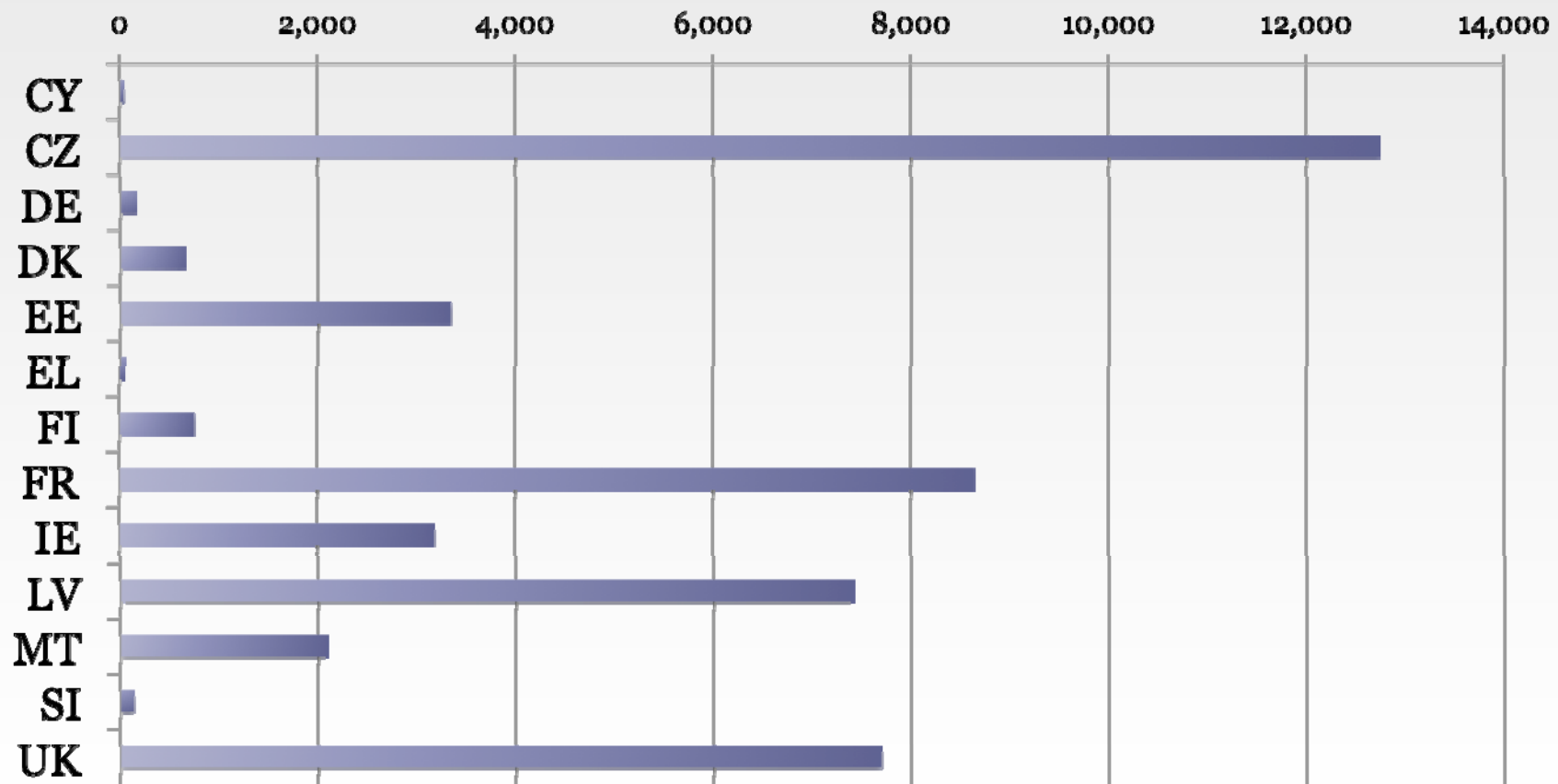


Data Retention Directive (2006/24/EC)

- §1(1) “This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime”
- *“The decision to retain communication data for the purpose of combating serious crime is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish.”* –Article 29 WP Opinion 3/2006
- *“[70%] of all data are use within 0-3 months ... and [85%] within 0-6 months”* (EC review)



Comms data requests/m people in 2008



Data: European Commission review of Data Retention Directive; IMF World Economic Outlook



Recent national court decisions

- Bulgarian Supreme Administrative Court blocked remote Ministry of Interior access to data and security service access without a court order (11/12/08)
- *“the obligation to retain the data ... as an exception or a derogation from the principle of personal data protection ... empties, through its nature, length and application domain, the content of this principle”* –Romanian Constitutional Court, 8/10/09
- *“Given the rapid advance of current technology it is of great importance to define the legitimate legal limits of modern surveillance techniques used by governments... without sufficient legal safeguards the potential for abuse and unwarranted invasion of privacy is obvious”* –Irish High Court, 5/5/10, making reference to EU Court of Justice



European contrasts with the US

- Stronger constitutional focus on privacy and data protection
- Heavier regulation of ISPs and other intermediaries – for data protection (“horizontal effect”), data retention, blocking of child abuse images
- Less of a bright line of protection for free speech:
 - Acceptance of *ex ante* censorship without judicial proceedings, or notification of blocked website
 - Sweeping restrictions on racist and xenophobic materials, genocide denial
- Digital copyright regime extremely similar (DMCA provisions echoed in Copyright Directive, minus put-back provisions)



References

- Douwe Korff and Ian Brown (2010) *New Challenges to Data Protection*. Luxembourg: European Commission.
- Ian Brown (2010) Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology* 19 (2) 95-109.
- Douwe Korff and Ian Brown (forthcoming) *Social media and human rights*. Strasbourg: Council of Europe Commissioner for Human Rights.