THE UNITED KINGDOM OF GREAT BRITIAN

ARTICLE 19’s Submission to the UN Universal Periodic Review

For consideration at the thirteenth session of the UPR Working Group, May 2012

Executive Summary

1. ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19) is a UK-based international, non-governmental human rights organisation established in 1986 that works around the world to protect and promote the right to freedom of expression and information, including by making submissions to the UN on countries’ performance in implementing established freedom of expression standards. ARTICLE 19 has observer status with ECOSOC.
2. With this submission, ARTICLE 19 seeks to make a constructive contribution to the preparation process of the UPR for the United Kingdom (UK). Given the expertise of ARTICLE 19, this submission focuses on UK compliance with its international human rights obligations in respect of freedom of expression and freedom of information, in particular:
   - Restrictive legislation relating to accessing information through the internet and other information and communications technologies;
   - Failure to reform defamation laws;
   - Continued misuse of the Official Secrets Act to limit public interest speech;
   - Excessive surveillance laws which allow for retention of information and monitoring of communications with little oversight;
   - Weaknesses in providing public access to information;
   - Po[illegible] including criminal defamation, blasphemy, and on implementation of the Freedom of Information Act, 2000.
3. These concerns are discussed in detail, followed by ARTICLE 19’s recommendations for actions to address them.

Limits on Internet Access

4. There has been a growing demand on internet services providers to limit access to content using various means. These restrictions are coming from both public and private sources. ARTICLE 19 is concerned that these efforts are chilling freedom of expression online and are being done without legal process.
5. The Digital Economy Act 2010 requires that internet service providers (ISPs) establish a 'copyright infringement list' of subscribers based on claims by copyright holders. ISPs are required to take technical measures against the subscribers, including slowing down or suspending their internet access completely, when they have been accused of infringing copyright a certain number of times. This process of determining the infringements takes place without any independent legal process before the decision is made and only limited appeals after. The Act also allows for copyright holders to petition a court to order the blocking of websites accused of providing access to a "substantial amount" of copyright infringing content.
6. ARTICLE 19 believes that the Act is a disproportionate response to the problem of online copyright violation. It creates a mechanism for restricting or suspending internet access which will have a wide impact, chilling the speech of individuals and households, well beyond that necessary for protecting intellectual property. It unfairly shifts the burden to subscribers to prove that they did not commit the infringement and that they took “reasonable measures”,

while not providing adequate safeguards for innocent providers or defining what the measures need to be taken. This creates legal uncertainty for subscribers which will result in innocent subscribers facing sanctions and many small providers stopping offering services. This will be especially problematic for those offering public internet access including libraries, schools and cybercafés.

7. There are also efforts to limit access to information and internet domains using informal processes. At the urging of the police, Nominet, the domain name register, is currently considering a new rule to allow it to freeze domain names at the request of police without a court order. According to Nominet, there were over 2,600 seizures of domain names between October 2008 and April 2011 conducted without court orders.
8. There have also been suggestions by authorities on limitations of social media. Following the London disturbances in 2011, Prime Minister Cameron suggested that police be given the powers to shut down social media sites and services.
9. There have been other recent incidents resulting in the removal of online content and the placing of restrictions on access to websites without legal authority:

    - Website Fitwatch.org.uk, which monitors police abuses, was taken down in November 2010 after a police officer acting without a court order contacted the web host and demanded its removal and the seizure of its domain name on the basis that it was "attempting to pervert the course of justice".

    - The domain name for website ihateryanair.co.uk, which provided public commentary critical of airline Ryanair, was seized based on commercial law claims in October 2010.

    - In January 2009, the Internet Watch Foundation (IWF), a group set up by ISPs to create a list of blocked sites, ordered the blocking of images in the Internet Archive's Wayback Machine, which prevented many UK-based users from accessing any of the 85 billion pages in the system.

    - ISPs reportedly regularly voluntarily take down materials under the Terrorism Act of 2006 when contacted by the authorities but no records are kept on the practice.

10. ARTICLE 19 believes that these cases show the weaknesses of the legal protections available to internet users and information providers where informal non-legal means are used to restrict access to information. We believe that all restrictions on access including takedowns, filtering, blocking and seizure of domain names need to be based on a legal process to be compliant with the ICCPR.

Defamation

11. In the 2008 UPR report, the Council recognised a substantial number of areas where UK defamation law infringes freedom of expression. These included "libel tourism", public figures, and conditional fees. There has been only limited progress in this area. ARTICLE 19 considers this lack of process to be a serious problem with profound effects on freedom of expression.
12. The Government introduced its draft Defamation Bill in March 2011 and it is expected to be considered in 2012. However, the bill does not address many of the problems noted by the Council in 2008. There is also currently a review and effort to reform fees. The European Court of Human Rights in Case of *MGN Limited v. The United Kingdom* (Application no. 39401/04), recently found that "success fees" violate freedom of expression. In addition, the courts have made decisions on jurisdiction and on enhancing protections for public interest journalism.

13. While the reforms and cases have been welcome, many problems remain. Libel is still frequently being used to stifle public debate on issues of important concern. Some of the recent cases include:

    - In January 2011, the NGO Soil Association was threatened with defamation for submitting comments in a public consultation opposing the opening of a new larger-scale pig farm.

    - The British Chiropractic Association brought a case against science writer Simon Singh for defaming its members in April 2008 after Dr. Singh wrote a column criticising many of their claims as lacking scientific evidence. The case was finally dropped in April 2010. However, Dr. Singh's legal costs were not fully covered, leaving him paying extensive legal fees.

    - Twitter was forced in May 2011 to identify anonymous individuals who had criticized officials at the South Tyneside Council. The case was brought by the Council using public money. While it was claimed that the allegations were defamatory, no further case was brought against the persons identified.

14. There is a particularly severe problem with defamation cases brought against internet users and intermediaries. Under the current system of notice and takedown, ISPs typically remove all material which has been challenged immediately out of concern of being held liable for the material themselves. There is no legal process and often this results in a large amount of material removed from online.

15. There is also continued problems over the issue of libel tourism where cases with little or no connection to the UK are brought in UK courts for defamation. In December 2010, the *Kyiv Post* banned access by UK-based individuals to their website following a case brought against them by a Ukrainian businessman. The case was dismissed in February 2011. International concern over the practice has resulted in the US Congress enacting the Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act in 2010 which prohibits UK libel judgements from being enforced in US courts.

16. There has been some positive developments which should also be recognised. The Criminal Justice and Immigration Act 2008 repealed the common law crimes of blasphemy and blasphemous libel and the Coroners and Justice Act 2009 repealed the criminal offences of sedition and seditious libel, defamatory libel, and obscene libel.

"Super Injunctions" and Prohibitions on Reporting

17. There were a number of cases where the courts issued injunctions prohibiting the disclosure of information by news media. In a number of cases, the court issued orders extending the publication ban to information that orders had even been issued, commonly known as "super-injunctions".

18. In 2010, the High Court prohibited the *Guardian* newspaper from publishing information, including on the injunction itself, relating to on the company Trafigura's dumping of toxic waste in Ivory Coast. Newspapers reporting on a parliamentary debate on the subject were also threatened.

19. Following the public revelation of these cases, the UK Government convened a review, chaired by Lord Neuberger, the Master of the Rolls, which recommended that their use be strictly limited.

20. ARTICLE 19 believes that "super-injunctions are a violation of Article 19 of the ICCPR and that all injunctions need to be strictly limited.

Official Secrets Act

21. The Official Secrets Act, which includes provisions originally adopted in 1911, criminalises the unauthorized release of government information in broad areas. In 2008, the Council expressed concern over its use to limit release of information of public interest and recommended it be limited in its use to cases where the information would be "harmful to national security." The recommendation followed previous recommendations in 2000 and 2001 from UN bodies on reforms to the Act to better recognise freedom of expression concern.
22. ARTICLE 19 believes that the OSA has been frequently used against government whistle-blowers and the media for printing information relating to the security services. In the past several years, the Act has been cited in controversial cases involving the public interest. These include:

    - In 2011, police demanded that *The Guardian* newspaper reveal the identity of confidential sources who provided information relating to police incompetence in their investigations of News International. The demand was dropped following public outcry.

    - In November 2008, MP Damian Green was arrested and his parliamentary offices searched by anti-terrorism police for receiving and releasing to the media documents from a source in the Home Office on poor performance on immigration.

Access to Information

23. The Freedom of Information Act 2000 and the Environmental Information Regulations 2004 set up procedural rules on access to information held by public authorities. The FOIA exempts all information from security services and also provides for a ministerial override. These exemptions allow for withholding of information in cases of important public interest including relating to torture and rendition.
24. There was also a serious concern about implementation, with excessive delays in both responses by public bodies and by the appeals body, the Information Commission. In the past year, there has been good progress in reducing delays at the Information Commission. However, there are continuing problems with many public bodies on providing access to information in a timely manner.
25. There also remain continued problems with individual access to their own records. Under Article 17 of the ICCPR, individuals have a right to protection of their family and personal life. The Council in General Comment 16 has stated that this includes a right to access and to correct personal information held by government and privacy bodies. The Data Protection Act, 1998 gives individuals a right to demand and correct information. However, there is no effective appeals mechanism. The Information Commissioner is not given the power to hear appeals in these cases even though it is the appeals mechanism for both data protection and FOIA. Individuals must bring cases before courts which is prohibitively expensive. This results in it often being easier to obtain non-personal information from public bodies. ARTICLE 19 believes that is a serious limitation to the right of information and the right of privacy as protected by the ICCPR.

Data Retention and Surveillance

26. ARTICLE 19 remains concerned about public authority use of surveillance to monitor communications as a violation under Article 19 and Article 13 of the ICCPR. The Data Retention (EC Directive) Regulations 2009 regulations require communications providers to retain communications data on all users for 12 months, including mobile-phone location and e-

mail logs. There is no requirement that the users are being investigated or even considered to have committed a crime and there are no exemptions for information that is otherwise protected, including that of the communications and mobile phone location data of journalists and their sources.

27. Government agencies access this information through the Regulation of Investigatory Powers Act (RIPA), which covers the interception of communications; the acquisition of communications data, including billing data; intrusive surveillance, such as on residential premises or in private vehicles; covert surveillance in the course of specific operations; the use of covert human intelligence sources like agents, informants, and undercover officers; and access to encrypted data. It requires that communication providers maintain interception capabilities, including systems to record internet traffic on a large scale.
28. RIPA allows national government agencies and nearly 500 local bodies to access communication records for a variety of reasons, from national security to tax collection. Orders for interception and access to content of communications require approval from the Home Secretary or another secretary of state, rather than an independent judicial officer. In 2010, there were 552,550 requests for communications data from telephone companies (including mobile-phone service providers) and ISPs. The law has been used against journalists to obtain their phone records and identify their sources in a number of cases.

Recommendations

29. In response to these concerns, ARTICLE 19 calls on the UN Human Rights Council to make the following recommendations to the UK Government:

- Repeal provisions of the Digital Economy Act which allow for the cutting off of internet users and the blocking of web sites;
- Ensure that all limits on access, blocking, filtering and takedowns of internet materials are judicially authorised and based on international freedom of expression exemptions;
- Reform the Official Secrets Act to only apply to cases involving substantial harm to national security. It should also be reformed to include a public interest defense;
- Reform libel law to including limitations on libel tourism, increase public interest defences and limit excessive fees;
- Repeal Data Retention (EC Directive) Regulations 2009;
- Reform Data Protection Act to ensure individuals have access to personal information held by public and private bodies.
- Adopt new rules which ban the practice of issuing “super-injunctions” which limit discussion that a case even exists.