

**BCS, The Chartered Institute for IT  
Consultation Response to:**

**Ofcom's Online Infringement of Copyright  
& the Digital Economy Act 2010 - Draft Initial Obligations Code  
Dated: 30 July 2010**

This page is left deliberately blank.

## **BCS, the Chartered Institute for IT**

The Institute promotes wider social and economic progress through the advancement of information technology science and practice. We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 70,000 members including practitioners, businesses, academics and students, in the UK and internationally. We deliver a range of professional development tools for practitioners and employees.

A leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

[www.bcs.org](http://www.bcs.org)

## Introduction

This is BCS, The Chartered Institute for IT's response to the 'Online Infringement of Copyright and the Digital Economy Act 2010: Draft Initial Obligations Code'.

The role of BCS under its Royal Charter is to work to bring about public benefit in the IT / Computing field, and this response is intended to reflect the professional view of the balance between the competing interests in this complex area. There are many overlapping rights and responsibilities, that while crystal clear in law and principle, compete and intertwine in the Digital Economy Act (DEA). The focus of this response is on ensuring that as attempts are made to protect the legitimate rights of copyright holders, 'collateral damage' is minimised.

This Code, in interpreting the Bill, creates some new definitions and obligations that are far-reaching; potentially affecting every household and business with an Internet connection. The Code as currently drafted reflects some thoughtful decisions about how to implement this in the most common use cases, but does not yet give confidence that important but less common use cases such as public wifi and community projects will be able to continue. Were these services to be negatively affected, this would be significantly against the interests of the public, and may well overshadow the benefit gained from curtailing illegal sharing of copyright material.

BCS would also like to recommend material on this topic from the Communications Managers Association (CMA) and JANET, who represent business and academic communications consumers very effectively. CMA is a part of the BCS group.

**Our responses to the Consultations questions (pg 40) are as follows:**

### Question 3.1:

Do you agree that Copyright Owners should only be able to take advantage of the online copyright infringement procedures set out in the DEA and the Code where they have met their obligations under the Secretary of State's Order under section 124 of the 2003 Act? Please provide supporting arguments.

*BCS is not commenting on this aspect.*

### Question 3.2:

Is two months an appropriate lead time for the purposes of planning ISP and Copyright Owner activity in a given notification period? If a notification period is significantly more or less than a year, how should the lead time be varied? Please provide supporting evidence of the benefits of an alternative lead time.

*BCS is not commenting on this aspect.*

### Question 3.3:

Do you agree with Ofcom's approach to the application of the Code to ISPs? If not, what alternative approach would you propose? Can you provide evidence in support of any alternative you propose?

*Regular reviews of where infringement is occurring are vital to ensuring that this is effective – both in terms of dealing with a migration of heavy infringers but also with relaxation of measures when infringement levels are reduced.*

### Question 3.4:

Do you agree with the proposed qualification criteria for the first notification period under the Code, and the consequences for coverage of the ISP market, appropriate? If not, what alternative approaches would you propose? Can you provide evidence in support of any alternative you propose?

*Yes, we believe that this is a pragmatic and proportionate approach that targets the vast majority of infringement while minimising potential negative impact on the market. Should this lead to a migration of heavy infringers, this could make enforcement more targeted and efficient.*

### Question 3.5:

Do you agree with Ofcom's approach to the application of the 2003 Act to ISPs outside the initial definition of Qualifying ISP? If you favour an alternative approach, can you provide detail and supporting evidence for that approach?

*The definition is for the most part useful, but there is an area where the detail could force a significant change to current practice. If all subscribers are required to identify themselves, this could have two effects:*

*Firstly, more vulnerable or excluded social groups may be less willing or able to make use of these services. Sometimes these services are essential for interacting with public services, but in general this would go against broader government objectives for digital inclusion.*

*Secondly, this requirement for identification could be seen as an erosion of civil liberties and an expansion of the 'surveillance society'. Again this would seem to flow against broader government objectives.*

*A pragmatic approach to this issue could involve exemptions that – as with other sensible and pragmatic decisions already taken in forming the Code – are easily dealt with as they do not affect the vast majority of subscribers.*

### Question 3.6:

Do you agree with Ofcom's approach to the application of the Act to subscribers and communications providers? If you favour alternative approaches, can you provide detail and supporting evidence for those approaches?

*No. This application is confusing in a way that risks the introduction of unpredictability into how individual undertakings will see the code applying to themselves.*

*It is also important to recognise the difficulties in defining 'measures' to secure a network in a way that is practical. In general, ISPs are able to employ top tier information security professionals to participate in the 'arms race' of online security. Individuals and undertakings may not be able to access and apply this level of expertise – and certainly not continuously.*

*Consequently, suggesting that those in this category 'take steps' presents a variety of potential problems; we are unsure what steps are reasonable to expect, or how this may interact with appeals. If not carefully considered, this could result in punitive action on the innocent, or easily-exploited loopholes. This uncertainty in and of itself could also create question marks around the existence and future development of innovative and useful services such as community wifi projects.*

**Ian Ryder**  
**Deputy Chief Executive**  
**BCS, the Chartered Institute for IT**