scripted

Volume 6, Issue 3, December 2009

Mandy and Me:

Some Thoughts on the Digital Economy Bill

Lilian Edwards[*]

DOI: 10.2966/scrip.060309.534

[*] Professor of Internet Law, University of Sheffield.

1. Introduction

So, once more unto the breach, dear friends, once more, where the breach is of copyright of course. First – a brief summary of the terrain.

Clauses 4-17 of the Digital Economy Bill introduce an "initial obligations" regime for Internet Service Providers (ISPs), whereby subscribers accused of filesharing by rightsholders will be sent warnings of alleged copyright infringements, or "strikes", by their ISPs; and a "technical measures" phase – to be green-lit only after evidence has been amassed that warnings do not work (but see below) – which will allow sufficiently warned offenders who still seem not to have seen the error of their ways to be disconnected from the Internet. Traffic slowing and banning of access to certain sites (e.g. the Pirate Bay), may also become available measures.

The Bill also, almost as an afterthought, adds a "***Henry VIII"*** clause, which allows the relevant Secretary of State (currently Lord Mandelson of ~~Mordor~~ sorry BIS) to make new copyright law in any area of Parts 1 and 7 of the Copyright, Design and Patents Act 1988 (CDPA), by statutory instrument (SI) – not primary legislation – if justified by speed of technological developments (even ones that have not happened yet – see proposed new s 302A of the CDPA.) So, essentially, new and important copyright laws (not exclusively to do with filesharing – Digital Rights Management, fair dealing and user rights might all be affected) are to be made under the public radar, and without proper Parliamentary scrutiny: anytime, anywhere (hereafter, the "Martini clause").

There has been a great deal of coverage of these matters – see e.g. ***here*** and ***here*** – so I will only point out a few matters of detail which have struck me as particularly worrying, on top of my well-ventilated previous concerns about the principle of a regime of "three strikes" at all. Most of the press attention has focused on the posited disconnection regime, since of course the sanction is so far reaching. But the warnings regime which, if the Bill passes, is likely to be of more immediate concern, is also staggeringly poorly drafted. This is where my focus will lie.

2. Accusations and Evidence

In the outline scheme we have, warnings are to be sent to subscribers solely on the say so of rightsholders. All a rightsholder need do, as presently laid out, is provide an IP address and time stamp of an alleged infringer to an ISP, and say that "it appears to [them that] a subscriber...has infringed the owner's copyright". There is no requirement this belief be objectively reasonable. Nor is there any apparent sanction for malicious or even simply careless or reckless allegations. Recent experience with the RIAA and BPI has shown that allegations made after IP address tracking at P2P sites often turn out to be wrong and that collecting IP addresses from P2P honey pots is a non-trivial exercise; so the issue of liability for erroneous accusations is an important one. Libel, malicious falsehood and data protection laws may offer remedies for the falsely accused; but there is no mention of such in the Bill itself (so far), nor of any reasonable duty of care. In other words, all the power is given to rightsholders, and none of the responsibility.

3. "Allowing Infringement"

The Bill also makes it clear that an infringement may be notified by a rightsholder if the subscriber "allowed another person to use the service and that other person has infringed". What does "allowed" mean here? It seems clear it is intended to cover the case where an Internet service is used to download by any member of the household other than the subscriber e.g. by partners, children, flatmates and lodgers – but what of casual visitors, friends of children? Should such persons be routinely policed by the subscriber fearful of liability, their rooms and computers searched, guests interrogated about their laptops and smartphones? What of Article 8 ECHR guarantees of privacy (which, let us remember, apply to children as well as adults, especially in their own bedrooms)? This is however only the start. What of the school or university or business which gives access to the Internet to hundreds or thousands of people? These warnings will come to roost at their doors, or rather their IP addresses. Will we then see IBM, Oxford University and Standard Life (just say) subsequently banned from the Internet? Is it really feasible to expect such organisations to stamp out downloading among all their employees or attendees (especially given most already do their best to try) or to spend the resources on internally trying to attribute the warnings to individual employees etc?

4. The End of Unsecured Wi-Fi?

A connected issue Pangloss has raised before relates to Wi-Fi. At present it is a subscriber's choice whether to secure their wireless network or not. Despite the public panic about paedophile use etc, many still think leaving Wi-Fi unsecured is a public service (see on this ***Daithi McSithigh's*** excellent piece). Yet one can easily see that leaving a network unsecured will count as "allowing" another's infringement (and note the mandatory requirement to notify alleged infringers about how to protect their Wi-Fi in proposed new s 124(5)(f)). What we see therefore is constructive prohibition of unsecured Wi-Fi by the back door, for consumers, corporations and the public sector (think of the impact on digital inclusion?); a decision of huge significance, which itself deserves a major public debate.

5. Appeals

Appeals against allegations untested in court and based on evidence solely of one interested party are vital. At the warnings stage, a single appeal is to be allowed, it seems, not to a full tribunal but merely to a "named person" who will be an arbiter of some type, independent of ISPs and rights holders, though not of OFCOM. Such an appeal is also vital to ensuring that this process meets the requirement of a "fair and impartial" hearing, ***under what was Amendment 138 to the now finalised Telecoms Package***. But no grounds are named in the Bill for an appeal against an erroneous warning to be allowed (there are some in relation to the better drafted and separate appeal against disconnection), nor is it stated what disposal the "person" could make if an error was found to have been made. Strangely, there is not even any requirement for alleged infringers to be told of this right of appeal, even though they are required to be given an enormous number of other pieces of educational "information". This is wholly unsatisfactory, especially in relation to Amendment 138.

6. Notification of Warning

Finally on this part, note (see proposed s 124A (7)) that warnings are to be deemed "notified" if sent to "the electronic or postal address" held by the ISP. As someone who never uses or checks their nominal ISP-provided email address (***mailto:something@virgin.net*** I guess), I would strongly suggest this be altered to "and" rather than "or". Of course this would cost substantially more to the rightsholders and ISPs, so possibly some midway solution should be found where an ISP is required to obtain a current used email address from its subscribers.

7. ISP Liability?

ISPs hold an unfortunate piggy-in-the-middle position in all this, forced by the threat of a fine of up to £250,000 to co-operate with rightsholders, even though they gain nothing from the process but overheads and customer ill-will. I have said ***elsewhere that I do not think it is just or sensible to enrol ISPs as "copyright cops"***, but if they are to be, they need strong protection from liability, ideally in the form of an indemnity from the rightsholders who actually plan to benefit from this whole stramash. ISPs face potential liability for sending out libellous allegations to subscribers, and again for disconnecting the wrong person on erroneous evidence, and in breach of contract, However currently all ISPs get by way of protection is the feather-light provision that an indemnity may – not must – be provided by the Code to be drafted (again, no further details now– see new s 124J (4) (b). If I were an ISP, I'd be going out now to price a shed load of legal liability insurance J - or to check out moving offshore.

8. The Disconnection Regime

Finally (gentle reader wipes brow), the present government has made a great deal of the assertion that ***the "disconnection" stage is a "nuclear deterrent" option*** – only to be implemented if all else has failed. One wonders why, three months before an election the current incumbents are likely to lose, it was not then simply left to the discretion of the next government whether to bring forward legislation, once the evidence was in. As it stands, the "disconnection" regime is supposed to be brought in, it has been widely reported, if a review by OFCOM shows (to some very vague timetable) that the "warnings and passing of ID details" approach is not working. However if you go and look, what s 124H(1)(b) actually says is that the Secretary of State may order that the "technical measures" stage may go ahead as appropriate in view of such a report OR "any other consideration". In other words, you can forget evidence based policy making if times are tough, and ***donations from rightsholders are needed***? Again Pangloss's suggestion would be for that last sub-clause to go.

I could go on – for most of a PhD length thesis I suspect – but enough is enough. This legislation bears every hallmark of having been drafted in haste on the back of an envelope on a wet Tuesday. It's so like **The Thick of It.** Only without the jokes.

PS: If you are unhappy with any of the above, can I politely direct you towards ***http://petitions.number10.gov.uk/dontdisconnectus/***?